“Mitigating the cyber security skills shortage:

The influence of national skills competitions on cyber security interest”

Tommaso De Zan

Linacre College

Department of Education and Centre for Doctoral Training in Cyber Security

University of Oxford

A thesis submitted for the degree of *Doctor of Philosophy*

Michaelmas 2021

Abstract:

There is a shortage of cyber security professionals in the current labour market, which is detrimental to countries' economic development and national security. Governments have attempted to deal with this issue by designing policies targeting both the supply and demand of cyber security skills. Among these policies, national cyber security skills competitions (NCSSCs) have been widely implemented to increase the pipeline of students entering the cyber security labour market. However, scientific studies on these interventions are scarce, and many questions are still unanswered: How do participants develop an interest in cyber security before joining a NCSSC? Do NCSSCs influence participants' interest in cyber security as a topic and as a career? What factors contribute the most to influence their interest? By answering these questions, this thesis aims to discuss the role of national skills competitions as a public policy to mitigate the lack of cyber security workers.

This research used the Italian NCSSC, the CyberChallenge.IT (CCIT), as a case study as it is the skills competition in Europe that provides cyber security training to the largest number of participants. This research employed a before and after design, collecting data from non-randomised comparison groups. Data were gathered following a mixed-method approach: quantitative data were collected through two online surveys and qualitative data through 50 interviews with competition participants.

This study found that CCIT students became interested in cyber security through a mix of “triggers,” most notably curiosity, formal and informal coursework, and the CCIT itself. Moreover, the CCIT increased interest in both cyber security as a topic and as a career. However, participants differentiated between the two, suggesting that theory should further investigate the relationship between interest development and vocational interest. Finally, this research recommends going beyond the concept of interest to fully appreciate NCSSCs’ impact, particularly by

including other relevant outcome variables, such as educational and career planning, key choices, and competing interests.

This thesis argues that NCSSCs organized and implemented like the CCIT could be a valuable solution to mitigate the lack of cyber security professionals. However, on its own, a skills competition programme is unlikely to achieve what a concert of policies might in dealing with the shortage. As the shortage issue has several roots, there are limits to what a NCSSC alone can do. However, it would lay a strong foundation for other policies to further steer students into the cyber security sector.

This thesis contributes to important debates such as interest theory, the relationship between skills competitions and interest, the design and implementation of NCSSCs and ultimately cyber security education and skills policy.

Acknowledgments

I would like to express my deepest gratitude to those who have been supporting me in this journey. This research would have not been possible without the help of and the opportunities given by the following individuals and organisations:

- My wife, my family, close and distant friends;

- My supervisors, Prof. Ewart Keep and Prof. Andrew Martin;

- The brilliant CyberChallenge.IT participants who accepted to be interviewed;

- Il Cybersecurity National Lab (in particular, Rocco De Nicola, Gaspare Ferrari and Paolo Prinetto);

- My examiners, Prof. Greg Austin, Dr. Craig Holmes, Prof. Susan James Relly, Prof. Ken Mayhew and Dr. James Robson;

- The Engineering and Physical Sciences Research Council;

- The European Union Agency for Cybersecurity;

- The Global Cyber Security Center;

- La Fondazione Mattei;

- (ISC)² and the Center for Cyber Safety and Education;

- The German Academic Exchange Service;

- The Centre for Doctoral Training in Cyber Security (in particular David Hobbs and Maureen York) and the Department of Education (in particular Velda Elliott) at the University of Oxford;

- Linacre College.

Contents

Acknowledgments 4
1. Introduction 10
1.1 Setting out the problem: the cyber security skills shortage and its implications 13
1.1.1 Evidence of failure in the cyber security labour market 13
1.1.1.1 The impact of Covid-19 on the cyber security skills shortage 17
1.1.2 The lack of cyber security professionals in Italy 19
1.2 Why a shortfall of cyber security workers is a concern 22
1.3 Thesis structure 25
1.4 Positionality statement 26
2. Literature review 30
2.1 Market failures, skills mismatches and policies 30
2.1.1 Market failures and skills mismatches 31
2.1.2 Government interventions 33
2.1.3 Summary and discussion 35
2.2 The cyber security skills shortage and public policy interventions 36
2.2.1 The causes of the cyber security skills shortage 36
2.2.2 Cyber security skills policies 38
2.2.2.1 Cyber security competitions as a policy to reduce the shortage? 40
2.2.3 Summary and discussion 43
2.3 Skills competitions 44
2.3.1 Skills competitions and theory 45
2.3.2 Cyber security skills competitions 50
2.3.3 Summary and discussion 54
2.4 The concept of “interest” 56
2.4.1 Definition and characteristics 57
2.4.2 Why is the concept of interest important for skills competitions? 58
2.4.3 The conceptualizations of interest 60
2.4.4 Measurement considerations 68
2.4.5 Summary and discussion 70
2.5 Skills competition and interest 71
2.5.1 STEM competitions and interest 72

2.5.2 Cyber security competitions and interest 74
2.5.3 Summary and discussion 79
2.6 Literature review summary and conclusions 81
3. Research questions and hypotheses 85
4. Methodology 90
4.1 Operationalisation: definition, context and choice of case study 90
4.2 The CyberChallenge.IT and the impact of Covid-19 92
4.3 Research design and methods 98
4.3.1 Research design 98
4.3.2 Research methods 100
4.3.2.1 Quantitative component 101
4.3.2.1.1 Outcome variable meAsurement and survey instrument 101
4.3.2.1.2 Data collection procedures 104
4.3.2.1.3 Quantitative data analysis 106
4.3.2.2 Qualitative component 109
4.3.2.2.1 Sampling strategy 110
4.3.2.2.2 Interview script preparation and pilot phase 111
4.3.2.2.3 Recruitment and data collection procedures 113
4.3.2.2.4 Qualitative data analysis 119
4.5 Ethics 122
4.6 Summary of methodology 125
5. The development of cyber security interest 128
5.1 Interest in technology and computer science 130
5.1.1 Videogames, school activities and access to technology 130
5.1.2 From videogames to computer science 132
5.1.3 Family members and their influence 134
5.1.4 Formal education and schooling 138
5.1.4.1 The rationale behind the choice of academic routes 141
5.1.4.2 Dissatisfaction with formal education and self-learning 143
5.1.5 STEM competitions 145
5.1.6 Early professional exposure 147
5.2 Cyber security interest formation in CCIT participants 150
5.2.1 Curiosity, internet browsing and readings 151

5.2.2 Coursework and conferences 152
5.2.3 The CCIT 155
5.2.4 Cyber security skills competitions 156
5.2.5 Key figures 159
5.2.6 Malware and cyber crime 160
5.3 Summary of findings 162
6. An assessment of cyber security interest before the CCIT 166
6.1 Interest in cyber security as a topic 166
6.2 Interest in cyber security as a career 171
6.2.2 The dream cyber security job: the penetration tester 178
6.2.3 "It is like the medical school of computer science": issues in cyber security educational and professional careers 179
6.3 Summary of findings 182
7. CCIT influence on cyber security interest and other variables 184
7.1 CCIT influence on interest in cyber security as a topic 185
7.1.1 Survey results 185
7.1.2 Interview results 187
7.1.2.1 Interview results: influence on CG participants 189
7.1.2.2 Interview results: influence on TG participants 192
7.2 CCIT influence on interest in cyber security as a career 195
7.2.1 Survey results 196
7.2.2 Interview results 198
7.2.2.1 Interview results: influence on CG 200
7.2.2.2 Interview results: influence on TG participants 202
7.3 CCIT influence on education and career planning 204
7.3.1 Education planning 204
7.3.2 Career planning 206
7.3.3 Difference between CG and TG 208
7.4 CCIT influence on educational and career choices 210
7.4.1 Survey results 211
7.5 Beyond cyber security: topic and career alternatives to cyber security 218
7.5.1 Survey results 218
7.5.2 Interview results 220

7.5.2.1 Artificial Intelligence 221
7.5.2.2 Programming and software engineering 222
7.5.3 CCIT influence on the relationship between cyber security and competing interests 224
7.6 Summary of findings 227
8. The CCIT programme 230
8.1 Reasons for signing up 230
8.2 The admission process 233
8.2.1 The appropriateness of the test 234
8.2.2 CG participants' feelings about the admission outcome 238
8.3 Inside the CCIT experience 241
8.3.1 The CCIT training 241
8.3.1.1 Training content and delivery 241
8.3.1.2 Relationship with professors 244
8.3.1.3 Relationship among students 245
8.3.1.4 The impact of Covid-19 on the CCIT training 246
8.3.1.5 A case study of a bad training experience 247
8.3.2 The skills challenges 248
8.3.2.1 June local skills challenge 249
8.3.2.2 October national skills challenge 250
8.3.3 CCIT and careers 252
8.4 Summary of findings 256
9. Is an NCSSC an effective solution to help mitigate the cyber security skills shortage? A discussion 259
9.1 Contribution to interest theory 260
9.1.1 Triggers of cyber security interest development: the role of curiosity and the CCIT 261
9.1.2 The relationship between interest development and vocational interest 264
9.2 A cyber security interest development system 266
9.2.1 Building the foundation of a cyber security workforce: the inclusion of cyber security formal education curriculums 267
9.2.2 NCSSCs as the cornerstone of a national cyber security interest development system 270
9.2.3 The labour market's role in mitigating the skills shortage 272
9.2.4 Skills competitions and the concert of cyber skills policies 275

9.3 The influence of a national cyber security skills competition on interest 280
9.3.1 The influence on cyber security as a topic 281
9.3.2 The influence on cyber security as a career interest 285
9.4 Is interest an adequate outcome by which to assess a national skills competition? 289
9.4.1. Educational and career planning 290
9.4.2 Key education and career choices 294
9.4.3. Competing interests and the “interest paradox” 298
9.4.4 Is *interest* still valid to gauge the impact of skills competitions? 300
10. Conclusions 302
10.1 Final summary 302
10.2 Limitations 307
10.3 Broader considerations 312
References 321
Annex I: List of acronyms 356
Annex II: Survey questionnaires 357
“Before” survey (February 2020) 357
“After” survey (October 2020) 364
Annex III: Reasons a regression discontinuity analysis would not work 371
Annex IV: Interview scripts 373
“Before” questionnaire (March 2020): 373
“After” questionnaire (October 2020): 376
Questionnaire for the control group 376
Questionnaire for the treatment group 378
Annex V: CUREC application form 382
Annex VI: Consent forms 401
Survey research information/privacy note and consent form 401
Interview consent form 406

1. Introduction

"*While billions of dollars are being spent on new technologies to secure the US Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success*."

(Executive Office of the President of the United States, 2009)

According to official statistics and anecdotal evidence from industry leaders and policymakers alike, there is a global lack of cyber security professionals in the labour market, the so-called cyber security skills shortage (CSSS). A recent report commissioned by the UK Government found that the country would need to attract approximately 17,500 new people each year into the cyber security sector to meet demand (Williams et al., 2021). Similar difficulties to fill cyber security vacancies have been reported in Australia, Japan and the United States (AustCyber, 2018; Ministry of Economy Trade and Industry, 2016; The Secretary of Commerce and the Secretary of Homeland Security, 2017).

Today's lives are heavily reliant on data, information systems and networks to the point that they can be considered the dorsal spine of modern economies and societies. Nonetheless, they are subject to cyber threats more than ever (The Council of Economic Advisers, 2018). Worried about the consequences of an insufficient number of people who can protect data and IT systems, governments have implemented various policies to increase the pipeline of cyber security professionals. For example, the UK government stated that "this skills gap represents a national vulnerability that must be resolved" and that it "will invest in a range of initiatives to bring about immediate improvements" (HM Government, 2016).

Interest in skills development is longstanding, and research on the topic has spanned a whole range of disciplines over the last half a century (Buchanan, Finegold, Mayhew, & Warhurst, 2017). As of today, however, scientific research has given little guidance on how to best deal with skills shortages (McGuinness,

Pouliakas, & Redmond, 2018). Most of this literature has been concerned with methodological issues regarding the incidence of skills mismatches rather than actual policy solutions to address them (CEDEFOP, 2015). Policy documents confirm this also applies to the cyber security sector (The Secretary of Commerce and the Secretary of Homeland Security, 2017).

Among the various policies implemented by governments to tackle the shortage, national cyber security skills competitions (NCSSCs) have been hailed as a practical and immediate solution. These interventions have been designed to tackle one of the issues currently compounding the shortage: increasing students' interest in cyber security in the hope they will join the cyber security sector. A recent Forbes article asked whether competitions can help close the cyber security skills gap and answered with no hesitation: "It's clear that these types of challenges are a good way to engage and inspire a new generation of cybersecurity pros" and therefore "challenges could be one highly effective way to bridge the gap" (Nachreiner, 2019). Even the Obama administration touted cyber security competitions "as a force multiplier for the STEM pipeline" (Polk, 2016). Nonetheless, whether this is the case is not so obvious, or at least, it has not been so thoroughly investigated. For example, the scientific literature warns that "despite substantial investment in cybersecurity competitions and a belief in their effectiveness in growing the cyber security workforce pipeline, we lack an understanding of how these programs affect occupational interest and professional engagement" (Tobey, Pusey, & Burley, 2014, p. 54). This seems true for the broader STEM (Science, Technology, Engineering, Mathematics) field, with a recent systematic review highlighting that it is unclear what kind of programmes are effective in preventing leakage of talent from science degrees (van den Hurk, Meelissen, & van Langen, 2019).

Against this background, this thesis sought to answer the following two main questions:

1) How do participants develop an interest in cyber security before joining a NCSSC? What factors specific to cyber security may trigger the development of such specific interest?
2) Do NCSSCs influence participants' interest in cyber security as a topic and as a career? If this is the case, what elements contribute the most to influence it?

By addressing these two main research questions, this thesis aims to discuss the role of national skills competitions as an effective public policy, especially when considered in the context of a broader strategy aimed at mitigating the shortage.

This thesis used the Italian NCSSC, the CyberChallenge.IT (CCIT), as its case study. It collected data before and after the skills competition using both quantitative and qualitative methods of data collection and analysis. It gathered data from non-randomized treatment and control groups that originated from the CCIT admission process. In the light of the research results, I will argue that an NCSSC organized and implemented in the same manner as the CCIT could be a valuable policy to mitigate the lack of cyber security professionals, especially if included in a wider policy system of cyber security interest development.

In addition to contributing to policy-relevant debates, this thesis also contributes to our current understanding of the concept of interest, especially the relationship between interest development and vocational interest.

The following sections expand on this introduction by describing the CSSS problem and why the lack of professionals is an urgent issue that governments may want to tackle (1.1 and 1.2). Following that, section 1.3 describes the main structure of this thesis. Finally, section 1.4 is about positionality, explaining how the idea of this research project came about.

1.1 Setting out the problem: the cyber security skills shortage and its implications

"(…) the cyber skills shortage is an ongoing challenge that needs to be addressed rapidly in order to mitigate some of the resulting issues (…); this also suggests that, left untreated, the extent of the shortfall will continue to worsen, as cyber security remains an area where demand for talent exceeds supply."[1]

(Williams et al., 2021)

This section provides evidence of the incidence of the cyber security skills shortage (CSSS), suggesting that issues currently affecting the cyber security labour market are hard to ignore. Various indicators are signalling a current shortage in national labour markets around the globe, and this section uses these indicators to show the problem's magnitude. This section comprises two subsections:

- 1.1.1 shows examples of indicators proving the existence of the CSSS in Australia, Japan, the UK and the US;
- 1.1.2 concentrates on CSSS indicators in Italy, where the chosen case study of this thesis took place, providing additional and more specific context to this research.

1.1.1 Evidence of failure in the cyber security labour market

Various indicators may signal the presence of a skills shortage and this section uses them to show the incidence of the CSSS in selected national labour markets. These indicators are:

- Shortage of workers
- Number and length of open cyber security vacancies

[1] This quote refers to an assessment of the UK cyber security skills supply in the period 2020-21.

- Rises in cyber security wages
- Employers and employees' opinions

The shortage of workers, measured as the difference between cyber security supply and demand, is among the key indicators showing the presence of a skills' shortfall. For example:

- In Australia, AustCyber, the organization tracking the national cyber security skills supply and demand, estimated that the number of new workers required is likely to be around 10,000 (AustCyber, 2020).
- A recent report published by the UK Government estimated an annual shortfall of approximately 10,000 people in the cyber security sector in 2021 (Williams et al., 2021). Furthermore, in 2019, in the first full review of the Shortage Occupation List (SOL) since 2013, the UK Migration Advisory Committee concluded that the cyber security specialist occupation was ranking "high" on shortage indicators and was the only one that should be added to the SOL among the ICT professions. According to the review: "The short-term mitigations have helped to fill shortages to some extent, but this has had limited impact as the skills required simply are not available" (Migration Advisory Committee, 2019, p. 189).

Other indicators showing the incidence of the shortage are the number and length of open cyber security vacancies, as well as the projected job growth:

- The Australian Department of Jobs and Small Business found that 42% of ICT security specialist's vacancies went unfilled in 2015, which is higher than the average recruitment failure of 33% in IT jobs. Furthermore, positions tended to stay open 20%-30% longer than for other IT roles. The Department also highlighted that only 1.7 applicants per post were suitable for these positions, the lowest figure in the entire IT sector (AustCyber, 2018).

- In the UK, a report identified 124,016 cyber security-related job postings between September 2019 and December 2020, with a demand for cyber security professionals growing by an average of 14% per annum since 2016. Of all the vacancies posted since the start of 2019, employers thought that 37% were hard to fill (McHenry et al., 2021; Williams et al., 2021).
- The US government had estimated the presence of 299,000 active openings for cyber security-related jobs in the United States as of August 2017, which grew to 464,420 in the period April 2020 – March 2021. A related analysis using the same online vacancy data found that cyber security vacancies took 20% longer to be filled than other types of IT vacancies (Burningglass, 2019; Cyber Seek, 2021; The Secretary of Commerce and the Secretary of Homeland Security, 2017). Moreover, as of October 2021, the Bureau of Labor Statistics considered the employment growth of the information security analyst career to be “much faster” (33%) compared to the growth of other computer occupations (13%) and the rest of the job market (8%) for the period 2020-2030 (2021) (figure 1).

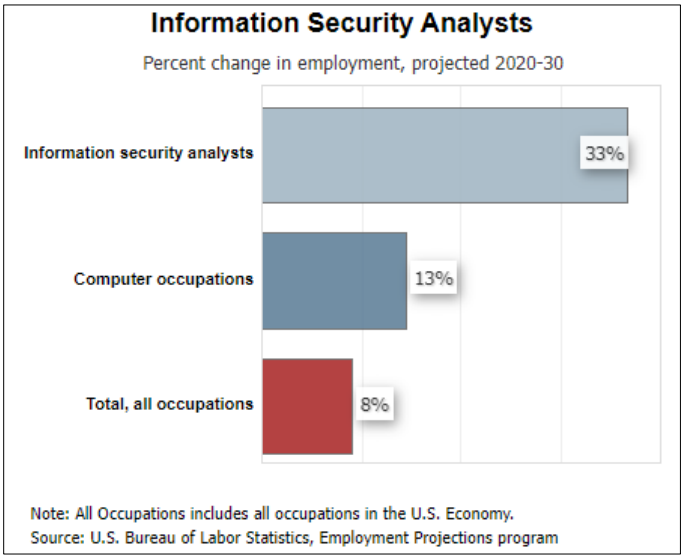

FIGURE 1 CHANGE IN EMPLOYMENT, INFORMATION SECURITY ANALYST CAREER (2020-30). SOURCE: (U.S. Bureau of Labor Statistics, 2021)

Cyber security wages have also been on the rise and have been comparatively higher than IT ones, which is another indicator one would expect to be under pressure if the sector was facing a shortage:

- In Australia, cyber security job wages have been growing by 2.7% per annum, 1% more than the annual wage growth for other ICT professions, and command an 11% premium over other digital occupations (Australian Cyber Security Growth Network, 2017). In addition, cyber security leadership and management roles can pay a premium of more than $20,000 above general IT management positions (AustCyber, 2018).

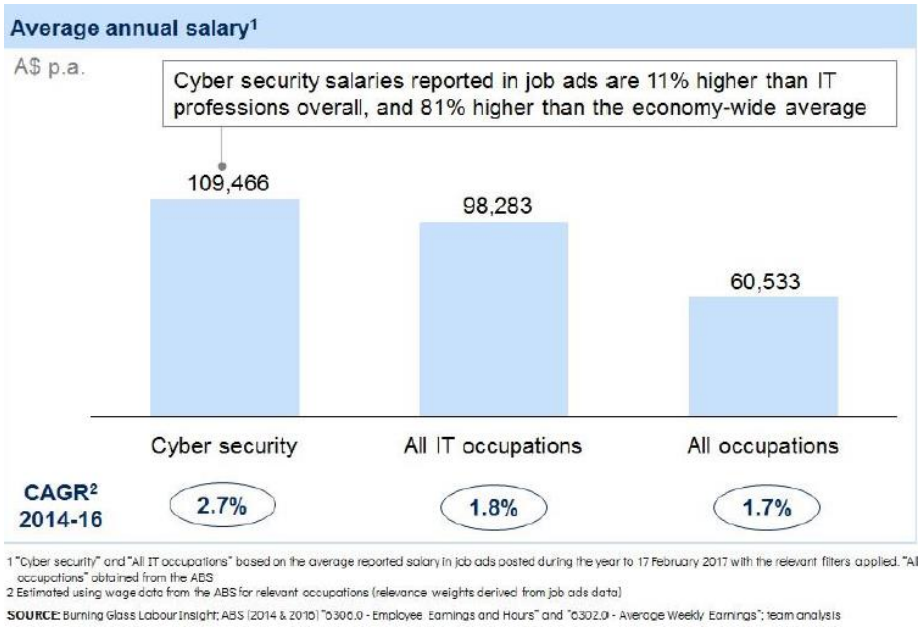

Figure 2: Average annual salary of cyber security occupations in Australia between 2014-2016. Source: Australia Cyber Security Network, 2017

- In the UK, the mean advertised salary was £59,200 (with a median value of £53,000) for a core cyber job posting in 2020, compared to a computer programmer who could receive a mean annual salary of £50,130 (with a

median of £41,078). This meant a wage premium of almost 30% for core cyber security jobs compared to IT jobs as a whole (McHenry et al., 2021).

- In the US, in May 2020, the median annual wage for information security analysts was $103,590 compared to $91,250 in the other computer-related occupations and $41,950 in all other occupations (U.S. Bureau of Labor Statistics, 2021).

Although industry research has generally been marred by methodological issues,[2] reports so far have unanimously concluded that: recruitment managers have been struggling to find cyber security professionals; vacancies have been kept open for a long time or remained unfilled; there has been an increase in the workload on existing employees; head-hunters have employed aggressive poaching tactics to recruit from competitors; and eventually companies have been losing proprietary data ((ISC)^2, 2018; Capgemini Digital Transformation Institute, 2018; Center for Strategic and International Studies, 2016; ISACA, 2015; Kaspersky Lab, 2016b, 2016a; Oltsik, 2017).

1.1.1.1 The impact of Covid-19 on the cyber security skills shortage

Approximately half of this research, including the entire online fieldwork/data collection process, took place in the midst of the Covid-19 pandemic. Covid-19 is an infectious disease caused by a severe acute respiratory syndrome named coronavirus 2 (World Health Organization, 2020). The virus was first located in the Chinese province of Wuhan in late 2019, but later spread globally in what has become known as the Coronavirus pandemic. As of October 2021, Covid-19 is thought to have infected 238,521,855 people, including 4,863,818 who later died (World Health Organization, 2021). To avoid spreading the disease, most countries worldwide restrained the movement of their citizens, who were often asked to stay

[2] These issues include non-randomization of the population surveyed, poor choice of indicators and doubtful quantification of the shortage at the international level (De Zan, 2019a).

at home, a decision that shuttered entire sectors of the economy. The IMF estimated that the global economy shrank by 4.4% in 2020, a decline that has been described as the worst since the Great Depression in the 1930s. In many countries, unemployment rates increased considerably, and vacancies hit historic lows (Jones, Palumbo, & Brown, 2021). While governments lockdown policies and the rollout of mass vaccinations have shown taming effects on Covid-19 in the second half of 2021, the pandemic will have long-lasting implications on societies, economies and labour markets (Shretta, 2020). In this context, it is worth asking whether something has changed regarding the cyber security supply and demand since this research started in 2017.

A first indicative element is that information security associations, which publish reports on the CSSS each year, reported no significant variations in how employers described cyber security recruitment and retention issues. More specifically:

- The 2021 annual report by Enterprise Strategy Group and Information Systems Security Association claimed that in 2020 the cyber security skills shortage had had an impact on 57% of organizations, stating there has been no “significant progress” toward a solution to this problem in the last five years (Oltsik, 2021);
- Similarly, the Information Systems Audit and Control Association found that 55% of organisations had unfilled cyber security vacancies in 2020, with 60% of employers waiting at least six months to find a suitable candidate (ISACA, 2021).
- Finally, the 2021 $(ISC)^2$ Cybersecurity Workforce Study stated that the global cybersecurity workforce needs to grow 65% to effectively defend organizations’ IT assets ($(ISC)^2$, 2021).

Moreover, a study of the UK cyber security labour market demonstrated that online vacancies for cyber security core roles decreased by one third between March and April 2020. Nonetheless, their number rebounded to pre-pandemic levels by Autumn 2020, suggesting that “despite the economic impact of COVID-19, there remains strong demand in the UK for cyber security professionals” (Williams et al.,

2021, p. 49). The shift to remote working meant a significant change for cyber security teams, who had to endure pressure to secure networks and larger attack surfaces while ensuring business continuity ((ISC)^2, 2021). However, these changes also meant that cyber security managers could argue for increased training and extra investment in personnel (McHenry et al., 2021).

Whereas it is perhaps too soon to have a full understanding of the impact of Covid-19 on the cyber security labour market and the skills shortage, the limited available evidence suggests that changes to the nature of cyber security work have not reduced demand for cyber security professionals, whose skills continue to be rare in the post-pandemic labour market.

1.1.2 The lack of cyber security professionals in Italy

The cyber security sector in Italy is affected by the same issues that Australia, the UK and the US are experiencing, even though there is usually less evidence than in these countries.

The CSSS was acknowledged for the first time in an official policy document in February 2018, when the Security Intelligence Department, which was the central institution in the Italian cyber security institutional architecture until the establishment of the National Cybersecurity Agency in 2021 (Dominioni, 2019), admitted that in Italy there was a "vast problem in relation to cyber security education" (Presidenza del Consiglio dei Ministri, 2018). Awareness about the issue was reiterated in late 2021 by the new chief of the National Cybersecurity Agency, Roberto Baldoni, who stated that "we do not have many competencies, neither in Italy nor in the world. There is a very big skills gap in cyber security, and this is one among many issues that add up to the number of cyber attacks" (Vivaldelli, 2021). Later in the year, he argued that the country would need approximately 100,000 experts to satisfy public and private sector demand (Boccellato, 2021).

Written by the four most prominent Italian IT industry associations in collaboration with the Italian government, the 2017 Observatory on Digital Competencies ("Osservatorio sulle competenze digitali") argued that the most needed skills are those in ICT strategy, management innovation and cyber security. Especially in the context of Industry 4.0, cyber security specialists were considered among the five most sought-after professionals. While there were no specific data on the CSSS, the report found that the labour market was missing between 4,400 - 9,500 university graduates in ICT-related subjects and had a surplus of between 5,200 - 9,500 high school leavers in the period 2016-18 (Aica, Assinform, Assintel, & Assinter, 2017).

The 2019 Observatory found that, in 2018, the information security manager and specialist were among the ICT professions with most open vacancies on the web. It also reported that a security engineer in a non-managerial position had on average an annual gross salary of almost €37,000, compared to an average of €32,000 in other ICT jobs. Furthermore, among 18 ICT fields, cyber security was in the top five areas where companies perceived they should get more training (Aica, Anitec-Assinform, Assintel, & Assinter Italia, 2019).

Finally, a survey sent to 45 relevant Italian cyber security organizations further underscored challenges in the national labour market. The overwhelming majority of respondents (80%) reported that their organizations "always" or "often" had cyber security vacancies which they struggled to or could not fill (figure 3).

FIGURE 3 SOURCE: (De Zan, 2019b)

When asked how many candidates applying to a position possessed the minimum knowledge and experience requirements, 60% of respondents said that either companies hired candidates who were not qualified or had difficulties finding even one competent professional. Moreover, 53% of organizations reported that cyber security positions were kept open for at least two months, if not longer, suggesting that cyber security roles were indeed hard to fill (De Zan, 2019b).

In line with what was found in the previous section on the impact of Covid-19, the Italian cyber security labour market has been reconsolidating in Italy as well, with online vacancies for information security managers and specialists growing at a steady pace in the second half of 2021 (table 1).

TABLE 1 NUMBER OF ONLINE VACANCIES PER QUARTER

Information security manager			
2020 Q2	2020 Q3	2020 Q4	2021 Q1
104	138	147	193
Information security specialist			
2020 Q2	2020 Q3	2020 Q4	2021 Q1
353	327	404	486

1.2 Why a shortfall of cyber security workers is a concern

"We are struck by the Government's apparent lack of urgency in addressing the cyber security skills gap, which is of vital importance to both national security and the economy."

(The Joint Committee on the National Security Strategy, 2018, p. 7).

As cyber security is about the "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation" (Department of Defense, 2007, p. 17), the lack of cyber security professionals has become a central issue for both governments and businesses.

Our lives are heavily reliant on data, information systems, and networks to the extent that it is not bold to claim that much of our life occurs online in today's ultra-connected world. From watching TV series on Netflix to chatting on Facebook with a friend living in another continent, it is hard to imagine a "disconnected life." Today, the data economy is behind innovations in machine learning, artificial intelligence and automation, and in the European Union, the value of this market reached 65 billion euros in 2017, with a €336 billion impact on the region's economy. The scale of data production is so vast that if we were to print every piece of data generated, we would produce nearly 1 billion 200-page books per second (Hoi Wai, LaFleur, & Rashid, 2019). Modern ICT technologies are the main drivers behind the so-called "Information Society," a society in which creating, distributing, using, integrating, and manipulating information is a significant economic, political, and cultural activity (Sarrocco, 2002).

As societal reliance on information systems and data grows, cyber security could be considered a public good to be managed in the national interest (Taddeo, 2019; Žáková, 2018). Cyber space is a constitutive element of information societies, intertwined with the physical, economic, social and political facets making such

societies. In particular, system robustness has direct and indirect implications for the public interest within information societies as it allows critical national infrastructures to work and citizens to conduct their lives (Taddeo, 2019). Therefore, the security of cyber space is paramount to place societal and technological development on a solid foundation and create the conditions to allow digital technologies to deliver socially relevant outcomes (Taddeo & Floridi, 2018a). Lack of adequate cyber security has the potential to force backpedalling on the information revolution and squander the development of information societies (Floridi, 2016; Taddeo & Floridi, 2018b).

However, because of vulnerabilities in their design and production, data, information systems, and networks (i.e. cyberspace) are subject to threats more than ever (The Council of Economic Advisers, 2018). For example, the World Economic Forum (WEF) ranks cyber-attacks, data theft and a potential breakdown of critical information infrastructures among the most significant risks the world faces (World Economic Forum, 2019). Similar concerns on the impact of cyber (in)security are shared by security agencies around the world (Coats, 2019) and risk advisory firms (Bremmer & Kupchan, 2019).

TABLE 2 WEF GLOBAL RISKS 2019

WEF's Global Risks Report 2019		
Top 10 Risks by Likelihood	*Top 10 Risks by Impact*	*Top 10 Risks by Interconnections*
1. Extreme weather events	1. Weapons of mass destruction	1. Extreme weather events and failure of climate change mitigation and adaptation
2. Failure of climate change mitigation and adaptation	2. Failure of climate change mitigation and adaptation	**2. Large scale cyber attacks and breakdown of critical**

		information infrastructures and networks
3. Major natural disasters	3. Extreme weather events	3. High structural unemployment or underemployment and adverse consequences of technological advances
4. Massive incidents of data fraud and theft	4. Water crises	4. High structural unemployment or underemployment and profound social instability
5. Large-scale cyber attacks	5. Major natural disasters	**5. Massive incidents of data fraud/theft and large scale cyber attacks**
6. Man-made environmental damage and disasters	6. Major biodiversity loss and ecosystem collapse	6. Failure of regional or global governance and interstate conflict with regional consequences
7. Large scale involuntary migration	**7. Large scale cyber attacks**	7. Extreme weather events and food crises
8. Major biodiversity loss and ecosystem collapse	8. Breakdown of critical information infrastructures and networks	8. Failure of major financial mechanism or institution and asset bubble in a major economy
9. Water crises	9. Man-made environmental damage and disasters	9. Large scale involuntary migration and interstate conflict with regional consequences
10. Assets bubbles in major economies	10. Rapid and massive spread of infectious diseases	**10. Adverse consequences of technological advances and large-scale cyber attacks**

There are various threat agents that cyber security professionals are tasked to protect cyberspace from, including cyber criminals, terrorists and hostile nation-

states, which all contribute to undermining online security (ENISA, 2018; European Cybercrime Center, 2019; Weimann, 2015). For example, cyber criminals have been targeting data and information systems for financial gains. According to some estimates, cyber crime has reached a total value at risk of $5.2 trillion globally in 2019-2024 (Ponemon Institute & Accenture, 2019). On the other hand, cyber terrorists have used ICT to spread propaganda, obtain funds to finance their operations and recruit new adepts. Although their capabilities have not reached the sophistication of other actors, their intentions remain intact and include attacking Western critical national infrastructures (Weimann, 2015). Finally, government agencies worldwide have been increasingly engaged in cyber operations to advance their strategic goals. State-sponsored cyber operations threaten international stability, and online disputes might have repercussions in the offline world, to the point that military organizations such as NATO would be ready to use physical force if the effect of a cyber attack was similar to an armed one (Stoltenberg, 2019).

In this context of increasing competition in cyber space, the lack of cyber security professionals who can protect cyber space might be considered a relevant threat to national security and economic development, which may warrant effective policy interventions to be redressed.

1.3 Thesis structure

In addition to this introduction, this thesis is comprised of 10 chapters:

- Chapter 2 reviews the literature forming the theoretical framework of this thesis;
- Chapter 3 formally states the research questions and related hypotheses;
- Chapter 4 describes the methodology, including methods of data collection and analysis;
- Chapters 5-6-7-8 presents the findings of this research;

- Chapter 9 analyses the findings in the overall context of the cyber security skills shortage;
- Chapter 10 concludes this research by presenting the study limitations and providing broader considerations regarding the future of cyber security skills shortage research in relation to some important contemporary debates.

1.4 Positionality statement

This section is about positionality and reflexivity, namely how "a researcher's background and position will affect what they choose to investigate, the angle of investigation, the methods judged most adequate for this purpose, the findings considered most appropriate, and the framing and communication of conclusions" (Malterud, 2001, p. 484). In this section, first, I discuss the process whereby I came to formulate this thesis' research questions; second, I position myself within the epistemological debate so as to be explicit about my beliefs when it comes to social science research; finally, I address the question of what research should be for.

I graduated from the University of Bologna with a bachelor's degree in political science and international relations and a master's degree in international relations. Because of this academic background, I developed an interest in public policy and international security issues.

After graduation, I started working at the International Affairs Institute in Rome. There, I had the chance to work on various projects at the intersection between technology and policy, including cyber security. While studying these issues, I noticed that the cyber security skills shortage was often mentioned as a policy problem that both industry and governments were struggling with. When I dug deeper, I realized there was a lack of solid scientific studies on the matter; hence, when I decided to pursue a PhD, I thought that the CSSS could be a good overall topic within which to identify a smaller issue to study in-depth.

The first year of my DPhil at the Centre for Doctoral Training (CDT) in Cyber Security was paramount to carve out my niche, particularly the possibility of exploring ideas with two "mini-projects." Very importantly, I could develop these ideas at the European Union Network and Information Security Agency, the EU Cybersecurity Agency, where I undertook a six-month placement between April and September 2019. There, given the doctoral research I was undertaking, I asked to be involved in some of the Agency's cyber security education and awareness projects, including the European Cyber Security Challenge (ECSC), the European cyber security skills competition. It was the blend of mini-projects findings and involvement in the ECSC that made me choose this thesis' research topic.

In the mini-projects, whose results were later unified in a single report (De Zan, 2019a), I argued that national cyber security skills competitions (NCSSCs) had become the most implemented policy worldwide with the objective of tackling the skills shortage. Nevertheless, I also warned that it was generally unknown whether these cyber security skills shortage policies, including NCSSCs, were achieving the intended goals, as governments had no evaluation mechanisms in place. In the meantime, attendance in ECSC's operational meetings had given me access to a network of competent and passionate competition organizers, some of whom were eager to further collaborate in order to understand the influence of their programmes. The methodology chapter will explain in detail why I selected the Italian skills competition as a case study.

During the research process, I went beyond my research topic and obtained a better understanding of the whole sector by engaging in various activities. For example, I continued collaborating with ENISA and produced research on cyber security skills development in the EU (De Zan & Di Franco, 2019) and identified key factors for the implementation of skills competitions (De Zan & Yamin, 2021). While collaborating with ENISA was also essential to continue funding my doctorate,[3] it was advantageous to gain a more comprehensive understanding of

[3] I received a fees-only scholarship from the CDT, but no contribution towards living expenses.

cyber security education, cyber skills policy and the cyber security labour market. Moreover, I also became involved in the Working Group on Cyber Security Culture and Skills of the Global Forum on Cyber Expertise, an international platform established to strengthen cyber capacity building and coordinate existing international efforts. There, I expanded my network of connections involved within cyber security education and better understood the implications that my research could have for policymaking and science, which also shaped how I interpreted research findings and conclusions.

A research project on national cyber security skills competitions in the context of the CSSS blends topics at the intersection between labour market economics, education and skills, cyber security and public policy. As I argued elsewhere (De Zan, 2021), this is not an easy topic for researchers to deal with as it requires multidisciplinary expertise. However, because of the mix of prior and newly developed knowledge, further research during my doctoral studies, and the professional networks I have been involved in, I consider myself to be in a solid position to contribute to these multiple debates.

Epistemology is about what is or should be regarded as adequate knowledge in a given discipline (Bryman, 2015). In this regard, while my epistemological beliefs are not as fixed and may change depending on the topic under investigation, I lean towards critical realism, a form of realism that recognizes the reality of the natural order and the events and discourses of the social world. The main thrust of critical realism is that we might understand and change those events and discourses only if we actively investigate the underlying forces that generate them, which can only be done through social science work (Bhaskar, 2013). Compared to positivists, who think that their conceptualization of reality reflects it in its purest form, critical realists believe that scientists' conceptualization is a way of understanding reality, implying that the categories scientists use to understand reality are provisory. Moreover, critical realists believe that it is crucial to understand the context in which regularities of the social world happen. Critical realism is *critical* in the sense that

the identification of generative/casual mechanism offers the possibility of introducing changes that may alter the status quo (Bryman, 2015). This epistemological predisposition had direct implications for the choice of data collection methods (ch. 4) and the reflections on the limitations of the research results (ch.10).

A final important matter that further elucidates the rationale behind this research is the question of what I believe research should be for. A purely academic perspective of social research would suggest that the primary scope of research is to add up to the stock of knowledge. However, for some social scientists, research should also have a practical purpose (Bryman, 2015). While I subscribe to the idea that social science research should often, if not always, tackle real societal concerns, I strongly believe that any policy should be based on scientific principles and evidence. While this might be obvious for many consultants or policy analysts in the business of scientific advice (Van Woensel, 2020), this might not always be reckoned by those writing laws and designing policies. This research topic is relevant within this debate as it clearly aims to tackle a genuine policy concern through the scientific method. Whereas the findings of this research contribute to advance theory in several ways, hopefully, readers will not be upset when this thesis invests time in explaining results with direct implications for practice too (ch. 10).

2. Literature review

This chapter reviews the research constituting the theoretical backbone of this thesis, pulling together various strands of social science literature – namely, labour market economics, skills mismatch, science education and cyber security. It is organized as follows:

- Section 2.1 explains why skills issues, including skills shortages, might arise as a result of market failures;
- Section 2.2 explains the causes of the cyber security skills shortage (CSSS) and the policies that have been suggested to deal with it; moreover, it shows the extent to which governments have resorted to cyber security competitions as a way to increase the pipeline of security professionals;
- Section 2.3 introduces the independent variable of this research, namely skills competitions; it first provides a general overview of these events and later delved deeper into cyber security specific competitions;
- Section 2.4 introduces "interest," this study's dependent variable with a particular focus on the conceptualizations of interest development and vocational interest;
- Section 2.5 links the previous two sections by exploring the literature analysing the influence of skills competitions on participants' interest;
- Section 2.6 summarizes this chapter and holistically discusses its main elements to guide the formulation of the appropriate research questions and hypotheses (chapter 3) as well as the methodology (chapter 4).

2.1 Market failures, skills mismatches and policies

This section situates the CSSS within the broader literature on market failures and skills mismatches, explaining why markets can sometimes produce suboptimal skills outcomes and why governments may therefore decide to intervene. Despite

the burgeoning literature on skills problems, skills shortages are under-researched and, because of that, we still know little about the best ways to remediate them.

2.1.1 Market failures and skills mismatches

Keep and Mayhew (1988) argue that skills issues arise depending on labour market dynamics, with various strands of economic theory providing different rationales for a range of outcomes. One school of thought posits that the market accurately depicts job demands, normally provides the right incentives and better adapts to variations in offer/demand than a non-market system. On the other hand, some economists are less optimistic about the intrinsic qualities of the market and recognize the possibility of failures, which occur when the market cannot achieve socially desirable results. This school of thought advocates government interventions to redress markets' imperfections. However, economists disagree on how extensive failures might be and how to best deal with them.

Keep (2006) summarizes four main reasons why markets fail:

I. Imperfect information: as employers and job candidates are not able to gather sufficient information on the content and quality of training provision, they struggle to reach optimal decisions or do not to understand the benefits of investing in different types and levels of training;
II. Short-termism and risk aversion: as investments in skills usually yield concrete results only in the long-term, individuals and employers are sometimes affected by short-termism, seeking a quick payback. Moreover, employers and individuals might also be risk-averse and decide not to invest in skills, whose returns are more complex to gauge than some other forms of investment;
III. Capital market imperfections: individuals may not invest because of economic constraints (such as having to pay a loan back), whereas employers might have difficulties in accessing credit and investing in skills;

IV. Externalities: externalities might take various forms, but the most straightforward is when a competitor poaches employees who have undergone training in different organisations.

Possibly more relevant in the context of this research, Holzer (2013) and Brunello and Wruuck (2021) concur that mismatches and shortages might materialize because of various cyclical and structural factors (i.e. globalization dynamics, ageing, business cycles etc.) but also when new technologies are introduced, and some types of skills are made obsolete in favour of new ones. Therefore, technology may change the nature of work (Ra, Shrestha, Khatiwada, Yoon, & Kwon, 2019) and create skills shortages by increasing the demand for skills that are not yet immediately available in the market. According to this theory, technological progress resulting from the spread of ICT have resulted in an acceleration in demand for skilled workers that has been not met by the available supply (Goldin & Katz, 2007; Katz & Autor, 1999).

The literature refers to skills mismatches when there are issues in the correct allocation of skills in the labour market. A skills mismatch can be used to describe various types of skills issues, including vertical mismatch (over-education vs under-education and over-skilling vs under-skilling), horizontal mismatch, skills shortages, skills gap, and skills obsolescence (Brunello & Wruuck, 2021; McGuinness et al., 2018).

Central to this research topic, skills shortages are a type of skills mismatch that ensue when there is a lack of qualified professionals applying to job vacancies despite employers offering market-level wages. Shortages are usually measured by unfilled or hard-to-fill vacancies. Measuring them is a challenge, and it is difficult to differentiate between genuine, over-emphasized or transient ones. Possibly because of this, shortages have not gained prominence: only 12 papers have been

found in the academic literature on this topic between 1994 and 2017 by McGuinness et al. (2018).[4]

Economists believe that workers and employers will adjust their behaviour when skills imbalances occur. However, this might take a comparatively long time: educational institutions might be late in reacting to employers' demands – for instance, through the establishment of new degrees or the expansion of existing courses – and, in doing that, increasing the pipeline of workers (Boeri & van Ours, 2008; Holzer, 2013). Mismatches might also take longer to be corrected as students lack information about the job market and cannot distinguish between high or low-demand professions (Chattopadhyay, 2012; Holzer, 2013). Other mismatches might be created by professions requiring skills that students find hard to or are not interested in acquiring. Finally, the education and training system might be unable to present an adequate educational offer that mirrors the needs of the labour market. Therefore, Holzer concludes:

> "if the failure of education and training […] to keep pace with skill demand among employers reflects market failures of some sort, then certain public policy interventions might be appropriate as remedies" (2013, p. 10).

2.1.2 Government interventions

When skills failures emerge, governments might decide to get involved. This is especially true for cyber security, considering the implications of successful cyber-attacks on economic development and national security (Bate, 2017; The Joint Committee on the National Security Strategy, 2018). Departing from the causes of how markets fail, Keep (2006) presents five general policy responses to this problem:

[4] Peter Cappelli gave a similar assessment: "It is difficult to think of a labor market issue where academic research…has played such a small role…where the quality of evidence and discussion has been so poor, and where the stakes are potentially so large" (2015, p. 223).

I. Exhortation and information on the benefits of skills' investments;
II. Establishment of employers' associations for the generation of skills as a collective good in order to avoid negative externalities (i.e. poaching);
III. Regulation, for example through the imposition of training levies;
IV. Assignment of property rights to overcome externalities and poaching;
V. Government's subsidy as a substitution for investments in skills.

Coming from the perspective of the more recent literature on skills mismatches, researchers and international organisations have compiled lists of policy options. These tend to differ vastly, usually depending on the target group, qualification level involved and nature of the skills mismatch. Despite this considerable policy variance, the literature appears to converge towards solutions such as:

- Career counselling and better information provision on employment growth and job vacancies (CEDEFOP, 2015; Furchtgott-Roth, Jacobson, & Mokher, 2009);
- Career-focused and technical education, for example in the form of apprenticeships (CEDEFOP, 2015; K. James, 2008; Lerman, 2010);
- Government-sponsored financial incentives to offer or fund training (CEDEFOP, 2015; Hollenbeck, 2008; OECD, 2017);
- Sector-specific training developed by employers and education providers (Edelman, Holzer, Seleznow, Van Kleunen, & Watson, 2011; Maguire, 2010; Roder & Elliott, 2011);
- New qualifications or adoption of new/modified curricula to close market gaps (CEDEFOP, 2015, 2018; OECD, 2017);
- Comprehensive national skills strategies based on skill-needs anticipation and constant monitoring and evaluation (Banerji et al., 2010; CEDEFOP, 2015; OECD, 2017).

2.1.3 Summary and discussion

To sum up, this section placed the cyber security skills shortage within the broader literature on market failures and skills mismatch. This review suggests that there might be different causes of market failures, and economists have long debated how and to what extent these occur. In the context of this research, one particularly relevant thread in the debate is the issue of how technological change can produce a demand for new skills that the available supply has yet to catch up with.

Within the skills mismatch literature, skills shortages have been under-researched, and studies have been primarily concerned with capturing their incidence rather than diagnosing their causes or how best to reduce them. While there is emerging literature on policy interventions, it is unclear to what extent these policies work. According to the European Centre for the Development of Vocational Training (CEDEFOP), “most skills mismatch research focuses on methodological issues, the incidence of mismatch and its impact, and not on actual policies and practices addressing it” (CEDEFOP, 2015, p. 6). The problem for skills shortages is even more accentuated as, among all skills problems, they are those with the most under-developed evidence base (McGuinness et al., 2018).

Finally, this literature is “generic” and possibly unable to capture the nuances surrounding the nature and features of sectoral shortages, such as the one in cyber security. Therefore, the following section goes deeper into the causes of the cyber security skills shortage and the policies that have been employed to cope with it. However, in line with the broader debate on skills mismatches and interventions, it will reveal that little is known about what has been successful in increasing the pipeline of cyber security professionals.

2.2 The cyber security skills shortage and public policy interventions

"The fact that wages seem to be rising for these jobs and the advertisements for them are increasing suggests that demand is greater than supply. […] What appears to have happened is that demand shot up very quickly; it takes students a while to get through education systems and to learn about the opportunity."

Anonymous interviewee (De Zan, 2019a, p. 22)

In addition to the above literature on market failures and skills mismatches, a stream of research has sought to directly engage with the current cyber security shortage and recommend policy mitigations. This literature is usually found in research reports from think tanks/research centres specializing in national security, rather than in peer-reviewed journals. These reports usually provide actionable recommendations on how to best deal with the CSSS, rather than a thorough analysis of the problem and its causes. Moreover, this literature highlights the role governments have entrusted to cyber security skills competitions in the hope that these interventions might influence students' interest in cyber security and make them join the sector.

2.2.1 The causes of the cyber security skills shortage

Bate unpacks the various issues that collectively add up to what she calls "the cyber security workforce development challenge." She argues that a net of inter-connected issues link together K-12 education, diversity and inclusion, higher education, industry certifications and competencies, recruitment, apprenticeships (or the lack thereof) in cyber security skills and education policy. She mentions three schools of thought on the current shortage: one thinking that the shortage is a function of simply not having enough people coming out of the education pipeline; the second believing that potential cyber security candidates and employers are not meeting because of the lack of strong matching mechanisms;

finally, the third school arguing that in a constrained hiring environment employers will seek their own solutions to fill jobs or reduce the number of employees needed. She posits that the workforce challenge is big enough for all these narratives to be at least partially correct in their diagnosis (Bate, 2018).

Building on this, De Zan (2019a) pinpointed four main factors concurringly compounding the CSSS. Two out of four pertain to issues within the demand side of the labour market. First, employers seem to have unrealistic expectations about the requirements candidates should possess to be hired in terms of years of experience, degrees and professional qualifications. For example, 89% of job postings in the US require at least a bachelor's degree, 75% at least between 3 to 5 years of professional experience and 59% at least one professional certification (Burningglass, 2019). These high-level qualification demands seem to be creating similar "labour market bottlenecks" in Australia (AustCyber, 2018). Second, employers are seldom keen to invest in cyber security human capital. At times, they appear to offer salaries below what a cyber security professional can command or provide unsatisfactory training opportunities to their employees. As an EU senior decision-maker put it: "The shortage is really dominated by a lack of understanding and adaption on our way of training people and fostering their development in the industry based on the way cyber security is evolving" (De Zan, 2019b, p. 37).

The remaining two factors relate to market failures concerning the education and training system as well as the pace of technological change. The first factor seems to be the inability of the education and training system to provide students with the tools to become a cyber security expert, mainly in terms of "right knowledge and skills" that employers look for in a potential employee. Issues that academic and industry stakeholders have found include: integrating cyber security in computer science degrees, promoting alignment between educational offers and labour market demands, developing multi-disciplinary expertise and encouraging educators to promote a more hands-on education (W. A. Conklin, Cline, & Roosa, 2014; Crumpler & Lewis, 2019; Gagliardi, Hankin, Gal-Ezer, McGettrick, & Meitern,

2016). The second factor seems to be the insufficient quantity of students entering academic and training paths that would make them more employable in the cyber security sector. For example, in the UK, 79,905 university students were enrolled in computer science degrees in the 2016-17 academic year, while 5,827 were in cyber security courses (Malan, Lale-Demoz, & Rampton, 2018), meaning that only 7% of IT-related students had a focus on cyber security. In Australia, there were only 1,150 enrolments and 231 completions from security science courses in 2017 and, according to organizations monitoring the national cyber security labour market, student demand needs "to increase significantly" to fill the number of places within the newly created cyber security courses (AustCyber, 2018).

2.2.2 Cyber security skills policies

As previously stated, rather than analysing the problem thoroughly, the literature in this field is usually keener on providing policy recommendations on how to increase the pipeline of professionals, supporting a rather interventionist approach. These recommendations advocate interventions at multiple levels, perhaps because it is recognized that different factors are concurrently begetting the shortage, requiring a comprehensive policy package to tackle all the dimensions of the problem. This is what Bate suggests, arguing in favour of a solution that should comprise "a network of connected policies and community-wide efforts" (Bate, 2018).

Policy recommendations can be divided according to the recipient of the proposed intervention, namely the education and training system (supply side) or employers and the labour market (demand side). Among the policies targeting the education and training system, reports usually recommend:

- Integration of problem-based learning in the classroom and the inclusion of industry practitioners in school faculties (Crumpler & Lewis, 2019; University of Phoenix, $(ISC)^2$, & $(ISC)^2$ Foundation, 2014);

- Implementation of a more rigorous curriculum (Crumpler & Lewis, 2019; CSIS Commission on Cybersecurity for the 44th Presidency, 2010), including how to ensure alignments between the educational curriculum and industry certifications/standards (University of Phoenix et al., 2014);
- Investment in new university programmes and incentivizes to encourage the establishment of regional hubs (Radunović & Rüfenacht, 2016);

Among the labour market policies or decisions that employers should implement at the firm level, reports usually suggest:

- Innovative hiring, acquisition and training practices and delineation of a cyber security career path as in other professions (CSIS Commission on Cybersecurity for the 44th Presidency, 2010);
- Support for internships (Crumpler & Lewis, 2019; University of Phoenix et al., 2014) and apprenticeships so as to blend educational models with work-based learning mechanisms (Bate, 2018).
- Hire with the intent of delivering on-the-job learning and external training (Aspen Cybersecurity Group, 2018), but also to retrain workers who show interest in cyber security (S. Cobb, 2016); and finally, consider ways in which the government and the private sector can collaborate in delivering training to students (S. Cobb, 2016; CSIS, 2016).
- ;
- Reconsider entry-level requirements, placing a greater emphasis on professional certifications and hands-on-experience (CSIS, 2016) while not being too fixated with degree requirements; write job descriptions that are aligned with existing frameworks such as the NICE Cybersecurity Workforce Framework (Aspen Cybersecurity Group, 2018);
- Enhance diversity in the cyber security field through the involvement of segments of the population that are under-represented, such as women, minorities and foreigners (CSIS, 2016);

Departing from this recommendation-based approach, De Zan instead reviewed how 12 countries have responded to the cyber security workforce problem (De Zan, 2019a). He found that governments have recognized the skills shortage as a challenge to their cyber security and elevated it to a policy priority. Most of the primary and secondary school interventions have been concerned with integrating and expanding cyber security teaching into existing curricula, teachers' professional development in cyber security, and the involvement of experienced industry personnel in faculties. Not many countries have tried to tackle the CSSS through vocational education or apprenticeship programs. Those who did usually established new degrees with a specific focus on cyber security and tailored them to the needs of the labour market. Efforts directed at the current workforce foresaw: establishing cyber security qualifications and certification schemes; promoting awareness initiatives for managers; expanding recruitment tools and retraining programs. However, governments have mostly tried to increase the pipeline of professionals by targeting the higher education systems. Policies vary depending on the country, but one can observe as recurring interventions the establishment of numerous scholarship schemes and new programmes or centres of excellence. Finally, a key tool in seeking to drive up supply has been the use of cyber security skills competitions.

2.2.2.1 Cyber security competitions as a policy to reduce the shortage?

Among this plethora of potential policy interventions, administrations have been particularly fond of cyber security competitions. Major countries now widely use cyber security competitions, which are possibly more widespread than any other policy instrument to tackle the shortage (De Zan, 2019a). These can be defined as "interactive, scenario-based events or exercises, in person or virtual, where individuals or teams engage in cybersecurity activities including methods, practices, strategy, policy and ethics" (NIST, 2018).

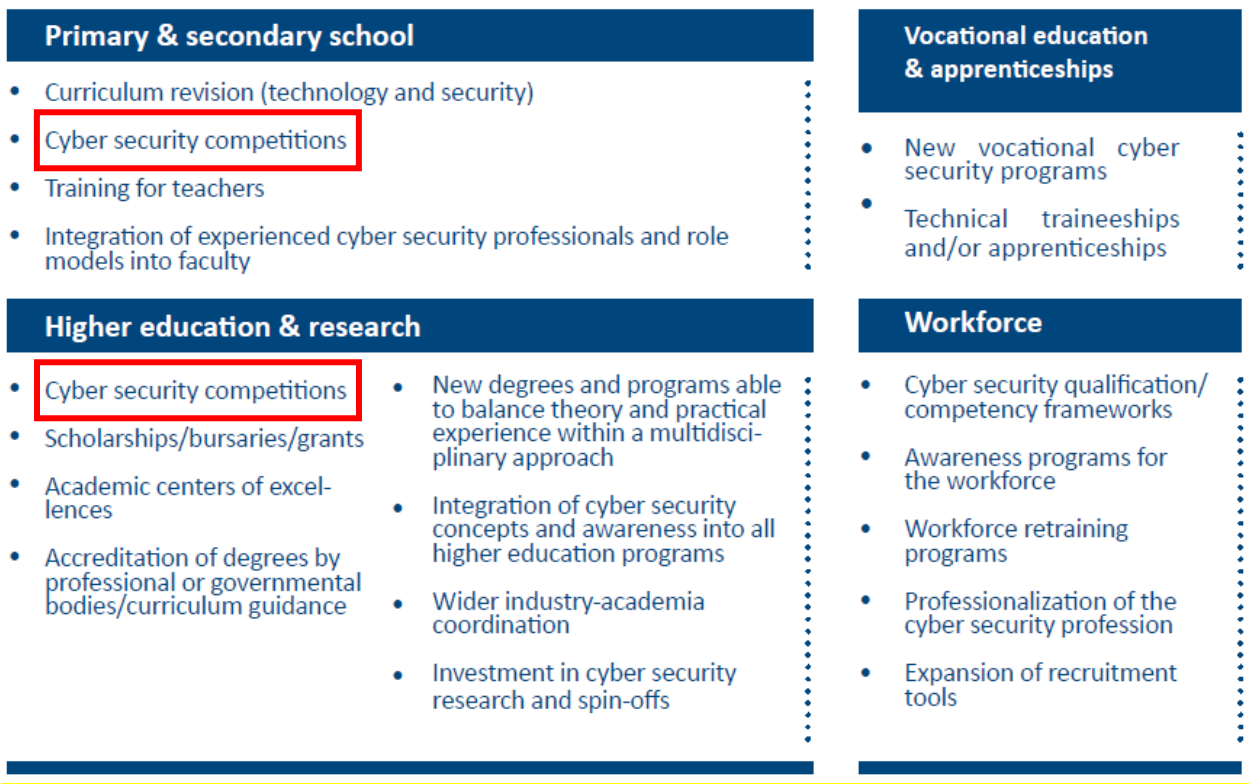

FIGURE 4 OVERVIEW OF CYBER SECURITY EDUCATION AND SKILLS POLICIES OF SELECTED COUNTRIES. SOURCE: (De Zan, 2019a)

For example, countries in the Five Eyes intelligence alliance and the EU have heralded cyber security competitions as effective solutions to: encourage young people to pursue a cyber security career, nurture students' interest, attract talented individuals to the field and, ultimately, meet cyber security skills demands while generating a self-sustained cyber security workforce (table 3). In this sense, cyber security competitions are thought to tackle one of the four main issues currently worsening the shortage: the low number of students enrolling in education and training pathways that could potentially increase supply. Because of that, competitions have been primarily targeting students in secondary school and undergraduate degrees.

TABLE 3 CYBER SECURITY COMPETITIONS KEY OBJECTIVES ACCORDING TO COUNTRIES IN THE FIVE EYES INTELLIGENCE ALLIANCE

Country and Author	Quote
Australia (Australian Government, 2016)	"Expanding the national annual Cyber Security Challenge Australia (…) will also help generate a sustained national pipeline of cyber security professionals."
Canada (CyberTitan, 2019)	"Youth are a vital talent pool to meet cyber security skill demands" and "This collaboration of National Youth Cyber Education Programs seeks to promote education and awareness in technology education and foster excellence in students pursuing careers in cyber security or other science, technology, engineering, and mathematics (STEM) areas."
United Kingdom (HM Government, 2018a)	The Initial Strategy cites Cyber Discovery as a program aimed at supporting skills capability "by identifying and engaging young people and nurturing their interest in cyber security as a future career path."
United States (The Secretary of Commerce and the Secretary of Homeland Security, 2017)	"Cybersecurity competitions have been increasingly popular tools for attracting talented individuals and federal agencies should make greater use of them, including for professional development."

Various examples of government-backed competitions are now an integral component of countries' cyber security workforce development strategies. Here we briefly describe those often used as case studies, which will be mentioned in sections 2.4 and 2.5 of this literature review.

For example, the UK Cyber Discovery is a government-funded extra-curricular programme for secondary students aged 13-18 to ensure that as many students as possible will enter the cyber security profession in the coming years (Cyber Discovery, 2019a). The program is among the policy interventions foreseen in the "Initial Cyber Security Skills Strategy" and has a budget of £20 million (HM

Government, 2019). It is designed around four phases, and students who score the highest in the various stages are invited to a final onsite boot camp and skills challenge. In the first 2018 edition of the programme, nearly 24,000 students signed up to the first phase; 170 were then invited to the final training boot camp (Cyber Discovery, 2019b, 2019c). According to UK government officials:

> "We need to inspire young people and show them a career in Cyber Security can be exciting and rewarding, not only to give them more opportunities but also help build a talented workforce for the future." (HM Government, 2018b)

Australia extensively deploys cyber security competitions, and CyberTaipan is among them. This cyber security competition is open to young students between 12-18 years old with an interest in cyber, defence, puzzles and code-breaking. The competition features several rounds, and the winning teams represent their school at the National Finals (AustCyber, 2019a). The organisers' objectives are to improve 1) awareness of and interest in cyber security careers and education pathways; 2) fundamental technical cyber security skills (AustCyber, 2019b).

In the US, the CyberPatriot program was introduced in 2009 to draw more young women and men to education and careers in cybersecurity and STEM fields. In the 2018-19 edition, 24,139 students participated in the cyber defence competition, significantly up from the 2010-11 edition when 3,635 students attended (Air Force Association, 2019).

2.2.3 Summary and discussion

To sum up, this section reviewed the literature on the causes of the cyber security skills shortage and potential policy mitigations. The literature recommends, and governments have implemented, numerous initiatives to reduce the shortage, mainly because multiple factors are compounding it. One of these factors is the low number of students pursuing cyber security academic degrees and professional careers. To challenge this trend, countries are increasingly making

recourse to national cyber security competitions, which have been primarily designed to spur interest in cyber security.

However, the problem with the policy solutions described in section 3.2, including cyber security competitions, is that there is little evidence about their effectiveness, in line with what was previously found by CEDEFOP (CEDEFOP, 2015). The research reviewed above either provides recommendations based on common sense – rather than, for example, an analysis of what has worked in other sectors – or a description of what countries have done, but rarely with any critical assessments of these interventions. However, because governments do not seem to have rigorous evaluation mechanisms in place,[5] and research has not yet fully pursued this line of inquiry, there is little or no evidence that any of these policies have ever worked (De Zan, 2019a).

Nonetheless, awareness among governments and researchers is emerging on the need to further investigate the policy solutions designed to mitigate the CSSS (Garcia-van Hoogstraten & Bate, 2019; HM Government, 2018a). Thus, it is essential to go beyond the mere description of policies and understand what could mitigate the lack of professionals. Specifically, knowing whether cyber security competitions are the right tool to reduce the CSSS is important as their use is widespread. Hence, the following section provides a more focused discussion on skills competitions.

2.3 Skills competitions

Section 2.2 concluded that governments have established NCSSCs to attract talented individuals to the field, nurture their interest and make them pursue a

[5] This has been candidly acknowledged by countries themselves. For instance, the US government stated that there is a "lack of rigorous evaluative information about the effectiveness of cybersecurity education and training programs" (The Secretary of Commerce and the Secretary of Homeland Security, 2017, p. 29).

cyber security career. In doing so, they have made them an integral component of their cyber security workforce development policy.

Using skills competitions to increase students' interest in a technical field is not new. In fact, they have become an increasingly popular Out-of-School Time (OST) activity over the past century to meet the growing demand for specialized technical workers (Miller, Sonnert, & Sadler, 2018). The National Research Council affirmed that OST activities have an essential contribution to make in promoting interest in science, "particularly to produce citizens literate in STEM concepts and to produce future scientists, engineers, mathematicians, and technologists" (Bell, Lewenstein, Shouse, & Feder, 2009; National Research Council, 2011, p. 5).

Before delving into the concept of interest, this review introduces skills competitions, the dependent variable of this thesis. It is organized as follows:

- Section 2.3.1 provides a general overview of skills competitions by describing their origins, the different theories underpinning them, examples of famous events and finally, their potential benefits and drawbacks;
- Section 2.3.2 explicitly elaborates upon skills competitions in the cyber security sector, their format and content, as well as the significant factors that supposedly make them successful;
- Section 2.3.3 summarizes and discusses the main elements of this section.

2.3.1 Skills competitions and theory

Historical origins

If the roots of education "lie hidden in an unknown past," the origins of skills competitions are even less traceable (Verhoeff, 1997), as competitions have long been used as a motivational tool for students across many disciplines and age groups (Fulton, Schweitzer, & Dressler, 2012).

In the late 1st century BC, a famous Roman teacher, Marcus Verrius Flaccus, is credited with introducing the principle of competition as a learning instrument. In

1984, the Eotvos University in Budapest established the first mathematics contest and from there, science competitions spread through Central Europe (Verhoeff, 1997). After that, competitions grew significantly in Germany, which developed the most elaborate national system with over 100,000 students involved each year in more than 20 federal competitions across several fields (J.R. Campbell, Wagner, & Walberg, 2000).

In 1934, the Soviet Union developed the first student Olympiad, organized as a series of examinations to identify the best mathematicians and encourage them to enter technical careers (James Reed Campbell & Walberg, 2010). In the US, interest in academic competitions grew after the Soviet Union launched Sputnik, and Edwin Teller, one of President Eisenhower's advisors, urged their development to channel students into scientific fields from an early age (Fulton et al., 2012).

Theoretical perspectives

Education theorists do not necessarily concur on whether competitive practices should be fully incorporated or not in the education system. One side postulates that competition is part of every culture, and since education should instil aspects of culture, competitive elements should be included in the school environment so that children can get used to them in later life. An opposing theory believes that competition does not encourage collaborative behaviour and hence it should be removed or at least minimized. Because of this dichotomy, the education system has had an ambiguous attitude towards skills competitions (James Reed Campbell & Walberg, 2010).

Another dichotomy is between social comparison and cognitive evaluation theorists (Nokelainen, Pylväs, & Rintala, 2019). According to the former, individuals feel the need to evaluate and improve their performances and minimize differences to the extent that one can argue that the purpose of competing is to evaluate the competence level of those involved (Garcia, Tor, & Schiff, 2013). By

contrast, the latter posit that the objective of the competition is to win extrinsic rewards (Nokelainen et al., 2019). As such, it has been assumed that the nature and duration of the competition and the maturity of students influence how a competition can elicit intrinsic and extrinsic motivation (Ozturk & Debelak, 2008).

There is no universal agreement among the proponents of competitions as to what objectives or structures competitions should have within education (Stanne, Johnson, & Johnson, 1999). Some argue that competitions constitute a break from traditional lectures, providing a change from the regular curriculum and teaching style. Others think that competitions effectively motivate students and provide feedback, implying that competitions should be based on the actual curriculum (Verhoeff, 1997). Moreover, competitions can be employed to develop the talent of the gifted (James Reed Campbell & Walberg, 2010).

Due to this multitude of potential goals and conceptualizations, skills contests can be classified using a taxonomy with several attributes and dimensions (Verhoeff, 1997).

Examples of popular skills competitions

Due to the increase in popularity of national skills events, international skills competitions have become progressively prevalent over the past decade (Nokelainen et al., 2019). There are now famous and internationally recognized skills competitions, which have been often mentioned in the literature as objects of investigation.

One of them is the global biennial WorldSkills Competition, “the gold standard of skills excellence,” organized by WorldSkills, which aims to inspire young competitors. WorldSkills is an opportunity for countries to benchmark their educational and vocational systems (WorldSkills, 2021). There are six primary skills areas in which contestants can compete:

- Manufacturing and Engineering Technology

- Information and Communication Technology
- Transportation and Logistics
- Creative Arts and Fashion
- Social and Personal Services

The latest WorldSkills took place in Kazan in 2019 and saw the participants of 1,354 young professionals representing 63 countries (WorldSkills, 2019).

More closely related to the focus of this research, another famous example is the International Collegiate Programming Contest (ICPC). Tracing its roots back to an event at Texas A&M in 1970, the ICPC is an algorithmic programming contest for undergraduate students. According to its organizers, it is the “oldest, largest and most prestigious programming contest on the planet” (ICPC, 2021). The ICPC is a multi-tier event encompassing local tournaments, regional contests, and world finals. In the past 20 years, the number of students attending this programme grew by 2000%, and, in 2020, ICPC Regionals saw the participation of almost 60,000 students from nearly 3,500 universities in 104 countries on six continents (ICPC, 2020).

Advantages and disadvantages of skills competitions

There have been two different schools of thought regarding skills competitions' practical benefits and disadvantages.

One is put forward by Wang and Yang (2003), who studied students’ motivation and incentives in a behavioural economic model. After including the educational psychology concept of self-worth into a traditional micro-economic analysis, they argued that a competitive learning environment might provide students with negative incentives. They explained that students compete for limited rewards such as good grades based on their performance. Performance is linked to potential self-worth and the perception of ability. Intense competition among students can cause concern and, when success is not guaranteed, failure is indicative of low ability, especially following a high effort. The result is that students

who are prone to negative self-worth might be discouraged. Hence, they argue that competition can be harmful if introduced into schools as an incentive. Similar arguments were put forward by Bandura and Locke, who suggested that an activity that emphasizes competitiveness may undermine the performance of those believing they are less capable, leading to a feeling of frustration or inferiority (Bandura & Locke, 2003; Cheng, Wu, Liao, & Chan, 2009; Kohn, 1986).

In a substantial departure from this theoretical economic perspective, the Modelling Vocational Excellence project analysed "the cognitive, affective, and social dimensions of expertise, and the processes through which such expertise is most effectively acquired" in the context of the WorldSkills Competitions (James Relly & Keep, 2019). In 2010, researchers surveyed 254 competitors and found that most of them enhanced their skills and enjoyed comparing them to those of other attendees (Nokelainen et al., 2019). Based on these premises, the Developing and Understanding Vocational Excellence (DuVE) project was established to further develop the practice of WorldSkills competition (Relly, 2016). The DuVE projects found that competitors are at the centre of the communities and organizations involved in these activities and are the primary beneficiaries of these events (Mayhew, Relly, Chankseliani, & Laczik, 2013; Nokelainen & Stasz, 2016). Furthermore, competitors receive training in the lead up to the competition, and when they return to their educational institution or employment, they spread new techniques and products into the system (James Relly & Holmes, 2012). Thus, the reach of the competition is more extensive, as employers witnessed improved performances as well as increased publicity and prestige, even with companies attracting more clients (Mayhew et al., 2013).

While this literature is useful to introduce the concept and practice of skills competitions, because the above studies refer to very different events from those this thesis seeks to investigate, it is beneficial to have a separate discussion on skills programmes happening in cyber security sector. This is undertaken in the next section.

2.3.2 Cyber security skills competitions

Definitions and goals

Cyber security skills competitions, defined as “interactive, scenario-based events or exercises, in person or virtual, where individuals or teams engage in cybersecurity activities including methods, practices, strategy, policy and ethics” (NIST, 2018), have been around for at least two decades. When Jeff Moss, the founder of DEFCON,[6] created the inaugural event in 1993 to convene hackers to speak about and share hacking skills in the same venue, the initiative gained traction (Ricci & Jessica, 2017).

In recent years, these skills competitions have been increasingly included in cyber security educational programs to introduce concepts and measure understanding of computer security and information assurance (Fulton et al., 2012; Hoffman, Rosenberg, Dodge, & Ragsdale, 2005). Nonetheless, due to their renewed role as a skills shortage mitigation policy, they have recently expanded in scope. A report of the EU Cybersecurity Agency found that European NCSSCs usually attempt to achieve five primary goals (De Zan & Yamin, 2021):

- Identify young cyber security talent;
- Increase interest in cyber security as a topic;
- Increase cyber security knowledge and skills;
- Increase interest in a cyber security career and connect participants with employers;
- Create a network of young cyber security specialists.

Content and structure

[6] DEFCON is one of the largest hackers’ conventions in the world.

Cyber security skills competitions can assume various forms and be focused on different types of activities. For example, Eagle (2013) described three main competitions' formats:

- *Individual and ladder-style problem sets*: participants compete individually and are given a chance to tackle a series of increasingly complex problems in a self-paced progression. Often, they cannot advance to the next stage unless they have solved a previous challenge.
- *Scored and problem-based*: these are often called jeopardy style. Organizers set a number of fixed problems with pre-assigned scores. The winner is the person or the team that scores the most points.
- *Team-based*: organizers install a closed network, and participating teams attack each other while simultaneously defending themselves against attacks. These attacks usually aim to steal a piece of information, which is called a flag (thus explaining why many cyber security competitions are called Capture-the-Flag (CTF) events), and submit it to the organizers for review. Teams receive points if they submit flags.

Besides their structures, cyber security competitions can also vary according to the nature of the skills challenges. After having analysed the competitions of major hackers conferences, Conti, Babbitt, and Nelson (2011) identified several topics and techniques, including:

- Network warfare
- Wireless
- Cryptoanalysis
- Hardware hacking
- Secure coding and malicious software
- Social engineering
- Physical security
- The arts

Nonetheless, as competitions have sprouted, their main characteristics and features have become more diverse. An ENISA report found that there is a great deal of variation in several key aspects, including team size, challenge categories, scoring methodology, hosting (online vs in-person), use of qualifier rounds, the inclusion of peripheral activities and communication channels for media strategy (van Rensburg & Baker, 2021).

What are the critical factors in a cyber security skills competition?

Taking into account the five main objectives that NCSSCs should aim to achieve,[7] organizers across Europe listed six main factors that are conducive to the "success" of these national events (De Zan & Yamin, 2021):

- the "policy relevance" of the competition
- a governance structure based on a public-private partnership
- appropriate funding
- a well-developed public relations and marketing strategy
- a training component to be paired with the actual competition event
- the presence of career awareness activities

Among these factors, two seem to be particularly relevant for this research: the cyber security training leading to the skills challenge and cyber security career awareness activities.

The training-skills challenge combo has been found to be effective in increasing students' knowledge and skills by other authors as well, often computer science professors involved in the organization of smaller-scale competitions organized at the local level. For example, Leune and Petrilli (2017) asked whether using cyber security skills competitions would enhance the "effectiveness" of cyber security

[7] Identify young cyber security talent; increase interest in cyber security as a topic; increase cyber security knowledge and skills; increase interest in a cyber security career and connect participants with employers; and create a network of young cyber security specialists.

education. Their study found that students were very engaged and spent considerable time trying to solve cyber security puzzles. Another question regarded whether students would develop stronger practical skills, which they did. Overall, they concluded that these programmes could improve cyber security education provided they are designed effectively.

Conklin (2005) affirmed that cyber security skills competitions should add a practical experience such as laboratory-based exercises, which help create an environment testing teams' knowledge. The importance of lab-based learning has also been underlined by Mullins, Lacey, Mills, Trechter and Bass in their experience with the Cyber Defense Exercise. They found that "the best way to teach network and system security is to explain the objectives, supply basic instruction, and then get the students onto the machines as quickly as possible" (2007, p. 48). They reported that their students enjoyed the hands-on, active learning environment of the lab and unanimously recommended to carry on with this type of learning method. A post-event survey found that 45% of students believed their cyber security knowledge came from the Cyber Defense Exercise.

McDaniel, Talvi and Hay (2016) used skills competitions to introduce high school students with no prior background to some computer security and digital forensics concepts. They found that using cyber security problems and tying them together in a competitive environment was "widely successful" at giving students foundational cyber security knowledge and motivating them to learn once the activity ended. They pinpointed four crucial elements in the design of these events:

- Challenges had to be accessible as frustrated students did not tend to continue with the camp;
- Offering help to students was critical as they were not always asking for it;
- Several students preferred to work in teams, especially as the challenges got more intricated;
- A gamified work environment was successful.

There is considerably less research on career-awareness activities organized as part of NCSSCs. In one study sampling skills competitions in Europe, national organizers deemed career awareness activities to be essential to link students with employers. A significant element was the creation of a network of individuals and organizations working in cyber security. The network could make possibilities in cyber security more visible and make it easier for participants to find relevant job placements after the programme. Moreover, networking events and career fairs were mentioned as suitable venues for connecting participants with employers (De Zan & Yamin, 2021). However, this study was descriptive and did not prove that these career awareness activities are directly responsible for increased cyber security interest among participants.

2.3.3 Summary and discussion

To summarize, this section introduced the dependent variable of this research, namely skills competitions, with a particular focus on cyber security events.

It is difficult to trace the origins of skills competitions, but what is certain is that they have been increasing in recent years as they are seen as a practical tool to motivate and inspire young people to become more involved in technical fields.

However, from a theoretical perspective, there are opposing views regarding the use of skills competition in educational settings, and this polarization has made educationalists adopt an ambiguous attitude towards them. If on one side, scholars believe that a competitive learning environment may provide negative incentives, on the other side, researchers have found that skills competitions can offer several benefits in the process of acquiring expertise and to the wider ecosystem. Different views resulted in a multitude of potential goals, conceptualizations and structures.

Cyber security skills competitions are placed within this broader framework and reflect this in some ways. As governments have started to use these events to mitigate the shortage of professionals, their features and scope have largely expanded. Notably, the literature has highlighted that training leading to a skills

challenge and career awareness activities are relevant factors when designing and implementing a skills competition, even though it has not yet proved whether they are also directly linked to an increased cyber security interest.

In the end, this section is valuable as it provides several elements that should be considered in a study on skills competitions:

- Research highlighted that competitions could yield both positive and negative consequences. Depending on the study variable, research on skills competitions must take into account its competitive nature, structure as well as objectives; it should also be open to the possibility that these programmes might have both positive and negative outcomes;
- One should be cautious in generalizing the findings of this literature as competitions' formats, contents, and aims are very varied. In other words, one should not conclude that, for example, a robotics competition focused on acquiring skills has the same effects as a cyber security competition whose goal is to increase interest in cyber careers. This implies that, when embarking on skills competition research, one should be clear about the study objectives and be aware of the context;
- Studies in these sections have been focused primarily on the role that competitions have in enhancing the knowledge and skills of participants. Therefore, a more focused discussion is needed to understand the potential role of skills competitions in influencing participants' interest. As this is the primary aim of this thesis, a separate section of this literature review (2.5) is dedicated to this;
- There is a need to better link competitions' objectives with means. Most competitions have now well-specified objectives, but whether these are achieved and how it is less clear. For example, while a cyber security competition might wish to increase interest in the topic and sector careers, how exactly and to what extent it does so is not evident when assessing the available evidence.

To find out, the following section gives an overview of the variable that cyber security skills competitions are supposed to influence in the context of this research, namely “interest.”

2.4 The concept of “interest”

According to interest researchers, educational policy has not devoted enough attention to triggering and maintaining students’ interest during the learning process. The presumption is that this is unnecessary as long as the education system teaches core knowledge and skills; moreover, manipulating interest through interventions is difficult and unlikely to succeed. However, interest research suggests otherwise (K. Ann Renninger & Hidi, 2020).

The concept of interest has often been associated with STEM subjects, particularly in analysing the exodus from science degrees in the 1970s. In this context, a study commissioned by the Department of Education in the UK (“The Dainton report: An inquiry into the flow of candidates into science and technology”) was particularly influential as it underlined a decline in the number of people entering science and engineering courses at university (Dainton, 1968).

This section reviews the scientific literature on interest, making extensive references to the work of Renninger and Hidi, who have pioneered and consolidated knowledge around this concept. This section is organized as follows:

- Section 2.4.1 defines interest and lists some of the features that distinguish it from other neighbouring concepts;
- Section 2.4.2 talks about the importance of interest, especially as one of the determinants of youths’ career choice;
- Section 2.4.3 deals with the various conceptualizations of interest, especially those related to interest development and vocational interest. Part of this section is also dedicated to interest “triggers;”

- Section 2.4.4 puts forward some measurement considerations, which gives pointers to establish an adequate methodology for this thesis;
- Section 2.4.5 summarizes this section, discussing crucial elements in the formalization of research questions, hypotheses, and methodology.

2.4.1 Definition and characteristics

Interest refers to a "cognitive and motivational variable that describes a) engagement, or participation, with some content and also b) the motivation to continue to seek opportunities to engage with that content: seeking information, posing questions, and tackling challenge" (K. Ann Renninger & Hidi, 2020).

The literature presents five characteristics of interest as an affect variable:

1. Content specificity (Krapp & Prenzel, 2011): the interest of an individual is always directed at something specific, be it an object, an activity, a field or a goal ("One cannot simply have an interest: one must be interested in something" according to Gardner (1996));
2. In recent theoretical developments, interest has been characterized as a phenomenon resulting from the interaction between an individual and his/her environment (Silvia, 2006);
3. Interest is characterized by both cognitive and affective components, even though the amount of each may vary depending on the phase of interest development (Mary Ainley, Hidi, & Berndorff, 2002);
4. Another critical aspect of the interest construct is its intrinsic character. Usually, an interest-related goal is compatible with the person's preferred values and ideals. At the same time, an interest coincides with willingness and readiness to acquire information and knowledge about a particular domain. Because of that, highly interested students possess a different knowledge structure about the domain in comparison to others (Krapp & Prenzel, 2011);

5. Interest has a physiological/neurological basis: one can notice a specific brain activity when a learner is engaged with interest and when she is not.

2.4.2 Why is the concept of interest important for skills competitions?

Developing and sustaining an interest has several positive benefits, including:

- heightening comprehension (Hagay & Baram-Tsabari, 2011);
- encouraging engaged work (Azevedo, 2013);
- influencing outcomes such as performance and course enrolment (Harackiewicz, Durik, Barron, Linnenbrink-Garcia, & Tauer, 2008);
- allowing people with low conscientiousness to meaningfully engage (Trautwein et al., 2015);
- making productive use of opportunities to choose from, such as picking the course students will continue to attend (Patall & Hooper, 2019);
- sustaining attention (M. A. McDaniel, Waddill, Finstad, & Bourg, 2000);
- helping to set and realize goals (Harackiewicz et al., 2008);
- promoting the use of effective learning strategies (Bernacki & Walkington, 2018);
- regulating behaviour (Sansone, C., Thoman, D., & Fraughton, 2015);
- and finally contributing to the feeling of self-efficacy (Lee, Lee, & Bong, 2014).

The effects of interest have also been studied in neuroscience. Interest fosters attention and learning, and when there is interest, effort follows (Dewey, 1913; W. James, 1890). Interested students are more likely to reengage with content by seeking specific information, and this type of behaviour activates the reward circuitry of the brain (Gottlieb, Oudeyer, Lopes, & Baranes, 2013). This dynamic has long and pervasive effects: it spurs attention (Anderson, Laurent, & Yantis, 2011), increases memory (Adcock, Thangavel, Whitfield-Gabrieli, Knutson, & Gabrieli, 2006) and energizes and motivates behaviour (Bunzeck, Doeller, Fuentemilla, Dolan, & Duzel, 2009).

Most importantly, in the context of our research, interest is thought to influence young people's career choices. In the context of Lent, Brown and Hackett's social cognitive career theory (1994), the authors advanced that interest, together with self-efficacy and outcome expectations, are key factors in influencing the choice goals that individuals make, for example, a person's desire to pursue a particular occupational path. Moreover, contextual supports and barriers encourage choice goals and actions 1) via direct paths, b) by moderating the relations of influence to goals and goals to actions, and c) indirectly via self-efficacy and outcome expectations (Sheu et al., 2010). More recent analyses have found similar positive correlations (Lent et al., 2018; Sheu et al., 2010).

Akosah-Twumasi and colleagues (2018) conducted a systematic review of factors that influence youths' career choices and found that the three major attributes that are likely to influence career choices are extrinsic, intrinsic and interpersonal factors. Each of these factors was further unpacked with sets of related elements:

- Extrinsic factors:
    - Financial remuneration
    - Job security
    - Professional prestige
    - Job accessibility
- Intrinsic factors:
    - *Personal interest*
    - Self-efficacy
    - Outcome expectations
    - Professional development opportunities
- Interpersonal factors:
    - Family members
    - Teachers/educators
    - Peers
    - Social responsibilities

Within the intrinsic factors, studies pointed to the role of personal interest in career decision-making, especially in the so-called individualistic cultures. For example, Bojuwoye and Mbanjwa argued that about 50% of youth career decisions are based on personal interests (Bojuwoye & Mbanjwa, 2006). Gokuladas posited that students from urban areas are more likely to make decisions based on their personal interests rather than societal ones (Gokuladas, 2010). Li et al. declared that, even in a collectivist culture such as the Chinese one, personal interest generates a significant influence, even though individual preferences are strongly connected to social comparisons (Li, Hou, & Jia, 2015). Atitsogbe et al. noted that Swiss students are also influenced by personal interest, and that interest differentiation was related to self-identity (Atitsogbe, Moumoula, Rochat, Antonietti, & Rossier, 2018). Choi and Kim compared Korean and American students' career choice drivers and revealed that Koreans seemed keener on including salary, job positions and promotions opportunities in their decision-making compared to peers in the US, who were led by personal interest (Choi & Kim, 2013). Finally, Caldera et al. also found that personal interest was linked to career aspirations in Mexican American women (Caldera, Robitschek, Frame, & Pannell, 2003). The issue of how interest generation impacts career choice in this research will be returned to in the later analysis chapter (n.10).

2.4.3 The conceptualizations of interest

There are different conceptualizations of interest, which reflect the vast range of alternative research questions that experts have tackled while seeking to solve related but different social dilemmas. In fact, Allport (1946) declared that "One of our greatest defects is our lack of a consistent or adequate theory of interest", and the situation has not yet changed (K. Ann Renninger & Hidi, 2011). Yet, despite this shortfall, there are at least five theoretically driven conceptualizations of interest that are worth noting, namely:

1. development (Krapp & Prenzel, 2011; K. Ann Renninger & Hidi, 2016)

2. emotion (M. Ainley & Hidi, 2014)
3. task features/experience (Sansone, C., Thoman, D., & Fraughton, 2015)
4. value (Eccles, Fredricks, & Epstein, 2015)
5. vocational interest (Lent & Brown, 2019)

In the context of this research, the most relevant conceptualizations are those related to interest development and vocational interest, which will be presented below.[8]

Interest development

Hidi and Renninger (2006) and Krapp (2002) are the reference authors for the conceptualization of interest development, described as a psychological state and predisposition to tackle specific content and re-engage with it over time in the context of a person's environment. Hidi and Renninger have focused on the relationship between interest and learning, while Krapp has been enthused about the relationship between interest and the developing self over time. Because Krapp's conceptualization of interest development is less relevant for this research, the paragraphs below are dedicated to presenting Hidi and Renninger's contribution.

Hidi and Renninger (2006) developed the Four-Phase Model of Interest Development, which comprises four stages of interest:

1. situational interest
2. maintained situational
3. emerging individual
4. well-developed individual interest

The process through which a new or an existing interest is created begins when something catches a learner's attention – a process called "triggering." When this

[8] For a review of the other conceptualizations, Renninger & Hidi provide a brief yet comprehensive overview (K. Ann Renninger & Hidi, 2011).

interest is *maintained*, repeated engagement with the content moves the interest from *situational* to *individual*. This engagement, which can be self-initiated or promoted by the environment, leads first to an *emerging individual* interest and later to a *well-developed individual* one. The authors describe the various stages as possessing different levels of affect, knowledge and value, even though measurements that can provide a more precise classification of these stages have not yet been developed. Below a summary table taken from Renninger and Hidi (2016, p. 13) presents the definitions of the model's stage and learners characteristics.

TABLE 4 PHASES OF INTEREST DEVELOPMENT

	Phases of interest development			
	Less developed		More developed	
	Phase I: *Triggered situational interest*	Phase 2: *Maintained situational interest*	Phase 3: *Emerging individual interest*	Phase 4: *Well-developed individual interest*
Definition of the stage	Psychological state resulting from short-term changes in cognitive and affective processing associated with a particular class of content	Psychological state that involves focused attention to a particular class of content that reoccurs and/or persists over time	Psychological state and the beginning of relatively enduring predisposition to seek reengagement with a particular class of	Psychological state and a relatively enduring predisposition to reengage a particular class of content over time

			content over time	
Learner characteristic	• Attends to content, if only fleetingly • May or may not be reflectively aware of the experience • May need support to engage from others and through instructional design • May experience either positive or negative feelings • May not persevere when with confronted with	• Reengages content that previously triggered attention • Is developing knowledge of content • Is developing a sense of the content's value • Is likely to be able to be supported by others to find connections to content based on existing skills, knowledge, and/or prior experience	• Is likely to independently reengage content • Has both stored knowledge and stored value • Is reflective about the content • Is focused on his or her own questions • Has positive feelings • May not persevere when confronted with difficulty • May not want	• Independently reengages content • Has both stored knowledge and value • Is reflective about the content • Is likely to recognize others' contributions to the discipline • Self-regulates easily to reframe questions and seek answers • Has positive Feelings

	difficulty • May simply want to be told what to do	• Is likely to have positive feelings • May not persevere when with confronted with difficulty	feedback from others	• Can persevere through frustration and challenge to meet goals

Vocational interest

Vocational interest is not a construct typically associated with interest research (Krapp, 2007; K. Ann Renninger & Hidi, 2011). The reference authors in this domain are Holland (1997), Johnson and colleagues (2004) and Lent and colleagues (1994).

Holland (1997) investigates the relationship between individual abilities with occupations (majors, training programs, etc.). He identified six characteristics related to the requirements of different occupations, namely being realistic, investigative, artistic, social, enterprising and conventional. However, this conceptualization of interest only captures whether interest is present or not at the time of the assessment. In addition, it does not address the issue of development or whether this interest might be supported or developed (K. Ann Renninger & Hidi, 2011).

In the context of vocational interest, Lent, Brown and Hackett's social cognitive career theory (1994) is probably the most relevant for this thesis. Building on the foundations of Bandura's (1986) and Hackett and Betz (1981), social cognitive career theory consists of five interrelated models, with the first focusing on the

determinants of educational and occupational interest.[9] Taken together, the five models have the goal of producing a unifying perspective on educational and career behaviour. In the first model on interest, the original research found that self-efficacy is substantially related to outcome expectations[10] (r=.49) and that the relationships between self-efficacy and outcome expectations with respect to interest were significant as well (r=.53 and .52, respectively). These findings suggested that the confidence in an individual's ability to succeed, rather than a more objective measure of competence or skill, was more likely to drive educational and occupational interest. These findings are confirmed by more recent meta-analyses (Rottinghaus, Larson, & Borgen, 2003; Sheu et al., 2010). In another recent meta-analysis focusing on interest in STEM, Lent et al. (2018) found that true score bivariate correlations of self-efficacy to outcome expectations (.49) and interests (.60) and of outcome expectations to interests (.58) were large in magnitude. Together, self-efficacy and outcome expectations were responsible for 46% of STEM interests variance, and both variables contributed similarly to the prediction of interest.

Triggers of interest

Another important line of research that falls outside the remit of those listed above is the literature on interest generation. This literature, grouped around what are termed either "sources" or "triggers" of interest, is concerned with the critical question of how interest is initiated. Researchers have identified an encompassing range of activities and tasks that contribute to interest generation, in addition to forms of self-formation, namely when interest comes directly from an individual.

[9] The second, third, fourth and fifth models focus respectively on career choice (see section above), performance, satisfaction and other well-being aspects in academic and career settings and the processes though which people manage development tasks and uncommon changes.
[10] "Outcome expectations are personal beliefs in the effect of an action on achieving a particular outcome. Outcome expectations are chiefly seen as being important in deciding to change behavior (i.e., the motivation phase)" (Lippke, 2017).

Activities and tasks. Mitchell's was one of the first studies differentiating between activities that could trigger situational interest from those that can maintain it. He discovered that working in teams and interactions with puzzles and computers were more likely to activate situational interest. On the other hand, personal relevance to the content and involvement were sources of maintained situational interest (Mitchell, 1993).

Building and extending the work of Mitchell, Palmer argued that novelty, meaningfulness and involvement were sources of interest in high school science classes (2004; 2009). Other authors also used Mitchell's work as a basis of their research and found that increased cognitive demand was linked to learners experiencing novelty, challenge, close attention and exploration, which resulted in increased situational interest (Chen, Darst, & Pangrazi, 1999, 2001).

Researchers have also investigated the importance of the structure, setting, facilitation and selection of activities. For example, Nolen stated that instruction that allowed students to connect with each other based on the content to be learned had a role in developing interest (2007). Using the classroom as the unit of analysis, Cobb and Hodge posited that when students assumed roles as data analysts to prepare arguments for a broader audience, it supported the development of a classroom-level group interest (2003).

Teamworking has also been found to promote the development of new interest. In two separate studies, Boekaerts and Minnaert noted that situational interest was linked to students' psychological needs for autonomy, competence and social relatedness and that situational interest and social relatedness could be found at each stage of group work (2003; 2007). Hidi, Weiss, Berndorff, and Nolan advanced the view that a powerful motivator of interest was being assigned the expert's role in presenting knowledge to the group during a science museum visit (1998).

An essential role in the initiation of interest is played by key figures such as parents, teachers and peers, especially when these key figures are central in creating the learning environment, designing the tasks, providing instruction and information,

as well as opportunities. In this framework, parents' and teachers' own interests cannot be overlooked (Dunst & Raab, 2006; Long & Murphy, 2005).

Self-generation of interest. In addition to activities and people, learners might be able to generate interest on their own, for example, when they use specific resources and information to engage with particular content. Sansone and colleagues were among the first to study the self-generation of interest, with research on undergraduates and how they were able to turn monotonous tasks into something interesting. A later study suggested that, when less interested, students used a strategy to make a task interesting, and this active action was a good predictor of continued engagement (Sansone, Weir, Harpster, & Morgan, 1992).

Moreover, Azevedo revealed that when learners have time, flexibility and develop a feeling of competence, they are more likely to self-generate interest (Azevedo, 2006).

Other studies reported that students might be able to self-generate interest if tasks were not challenging enough and that the learning environment can support them when they self-regulate in such activity. For instance, Meyer and Turner observed students in middle school actively increasing the difficulty of a writing assignment by writing more than was required (Meyer & Turner, 2002).

Finally, Hulleman and Harackiewicz described how students could be supported to self-generate interest if they are required to reflect on the value of the task. In their research, students linked their own lives with what they would be learning in the course, which was led by a self-generated explanation of value for semester-long courses. This process implied the triggering of interest, which became self-generated (Hulleman & Harackiewicz, 2009).

2.4.4 Measurement considerations

Reflecting this variety of conceptualizations, there currently is “no single correct measure or indicator of interest or interest development,” and such specification may never be found because of differences in disciplinary domains dealing with the concept (K. Ann Renninger & Hidi, 2011; K. Ann Renninger & Su, 2019). Many methods and tools have been used to measure interest development, including self-reports, behavioural measures and neuroscientific methods. Given the relevance to this research project, self-reporting is reviewed below.

Self-reports are the most common form of interest measurement and usually imply asking study participants to rate or comment on their interest level at a given moment. The questions asked can range from straightforward assessments of their interest such as “How interested are you in computer science?” to more complex ones that involve a deeper theoretical understanding of the concept such as “How likely are you to engage in computer science tasks that are not assigned in school?” In addition, surveys might include Likert-scale or open-ended questions.

The content of the items used for the investigation may vary a lot. Renninger and Hidi (2011) warned that the type and content of items that researchers use to make their assessment should be aligned with established theoretical perspectives and according to prior research findings. However, they noted that this is not always the case, with items disengaged from any specific conceptualization of interest, affecting data collection and interpretation.

In addition to the content, the structure of self-reports also tends to differ. For example, Alexander and Murphy researched interest in educational psychology by asking students to rate how much they liked 26 topics within the domain on a seven-point rating scale (1998). This type of measurement is clearly different from studies where interest is evaluated with Likert ratings including knowledge, feelings and activities and open-ended questions (K.A Renninger, Ewen, & Lasher, 2002) or four-hour-long open-ended interviews (Fink, 1998).

Regardless of content and structure, multiple sets of items and sources of information provide more evidence for the purpose of understanding the relationship between interest and other variables, as well as the trajectory of interest development. In fact, in-depth post-experience interviews with individuals have collected rich sources of information in specific populations (Fink, 1998). Likewise, surveys have also been helpful to understand changes in interest over time when the participant group is large or has not been studied yet.

Renninger argues that many researchers have evaluated interest by asking study participants to rate how much they like a particular content, which might be effective to understand whether interest is present or not, but it is unlikely to capture how much interest is developed. Thus, an assessment of the status of interest must consider its cognitive component. This is why Hidi and Renninger noted that the identification of developed interest must encompass a relation between feelings, value, knowledge and thus proposed four indicators that can be used to assess it (K. Ann Renninger & Hidi, 2016). In this assessment, one should find out how the study participant, compared to other activities and given the opportunity, will engage with the content or topic of interest:

1. frequently
2. with understanding or depth of knowledge
3. voluntarily
4. independently

Renninger and Schofield (2014) have found these four factors to form a single one (with $\alpha = 0.91$), which have been used to create methods for the collection of data using self-reporting and to distinguish among different phases of interest development (Michaelis & Nathan, 2015).

2.4.5 Summary and discussion

To sum up, this section reviewed the relevant literature on the concept of interest, including aspects, such as measurement, that are worth considering in the design of the methodology of this research.

This research adopts Renninger and Hidi's definition of interest, a cognitive and motivational variable that involves continuous engagement with specific content. Other critical aspects of the concept include the interaction between the individual and the environment, its intrinsic character shaped by a person's preferred values and ideals, willingness to acquire information, and its neurological basis as linked to the brain's reward circuitry.

Triggering and developing interest has numerous benefits, including guiding youth's career choices, which is relevant for this thesis. In fact, this study considers national cyber security skills competitions in the context of the shortage of security professionals. While it is important that these events increase interest in cyber security overall, policymakers also expect them to influence students' career choices (see section 2.2.2.1).

There are different conceptualizations of interest, but this thesis pays particular attention to those related to interest development and vocational interest, given the overall theoretical and policy framework. In particular, this research relies on the theoretical considerations of interest development made by Renninger and Hidi and the social cognitive career theory by Lent and colleagues; other relevant theoretical contributions are the studies on "triggers" of interest. Overall, as authors have noted the need to bridge research on interest development and vocational interest (K. Ann Renninger & Hidi, 2011; K. Ann Renninger & Su, 2019), this research may immediately contribute to this effort.

Another contribution this thesis wishes to make regards the specificity of the "interest" that it seeks to explore, namely cyber security interest. To the best of our knowledge, there are no scientific inquiries entirely devoted to studying cyber security interest, particularly how this is generated and developed in the first place

and how this is shaped by an intervention such as a skills competition. As content specificity is one of the main features of the interest concept, this research's findings may advance theory and provide actionable recommendations to tackle the shortage more holistically.

Finally, the last section described the measurement issues that should be considered when investigating interest. The literature review noted that there are currently no universally established measurements or protocols to study interest, mainly because of the various disciplines and research questions that have employed the concept of interest to tackle critical societal problems. Nonetheless, this does not mean that a study on interest occurs in an intellectual vacuum. Instead, a researcher should align his methodological instruments to prior conceptualizations and research findings.

2.5 Skills competition and interest

The previous two sections introduced the general literature on skills competitions and interest. While this literature provides a broader framework, it is perhaps too high-level to directly inform the relevant questions, hypotheses and methodology. Luckily, there is a niche literature on the relationship between STEM competitions and interest that includes studies specifically focusing on cyber security skills events. This research is helpful because section 2.3 noted that the significant content and organizational variance of these programmes are likely to generate different outcomes. Therefore, it is advisable to take note of the most specific research possible to correctly steer this thesis' research design. This section is divided into two parts:

- section 2.5.1 reports the results of the literature on general (i.e. other than cyber security) STEM competitions and interest;
- section 2.5.2 reviews studies on cyber security skills competitions and interest.

2.5.1 STEM competitions and interest

Welch and Huffman (2011) studied the extent to which after-school robotic competitions influenced students' attitudes towards science. Results were obtained from a sample of students who attended the First Inspiration and Recognition of Science and Technology (FIRST) robotics competition and a group of students from the same schools who did not attend. Students' attitudes were recorded before and after the programme using the Test of Science Related Attitudes. The statistical analysis detected no difference between the groups in relation to leisure interest in science or their aspirations for a science career.

Dabney et al. (2012) explored the links between OST activities and interest in STEM and related careers. They claimed that most studies do not reveal whether interest in STEM is the reason why students attend OST activities or a consequence of being involved in such activities. The Persistence Research in Science and Engineering survey was sent to a nationally representative sample of students enrolled in introductory English courses from 34 randomly selected U.S. universities and was completed by 7,505 students (62.5% response rate). Using a logistic regression model with career interest in university as the outcome variable, they found that those participating in OST clubs/competitions and reading/watching science content at least a few times a year were more likely to be interested in a STEM discipline at university, after controlling for demographic and background variables. They also discovered that students with higher socio-economic backgrounds were more likely to participate in OST clubs/competitions. However, the study aimed to measure the association between OST activities and STEM career interest at university and not establish causation. To further advance research on the matter, authors proposed to develop a longitudinal study investigating students' pathways to specific careers, controlling for variables such as pre-existing STEM interest, socio-economic status and gender.

Miller, Sonnert and Sadler (2018) sought to answer three questions: Does participating in STEM competitions increase interest in a STEM-related career at

the end of high school? Do specific STEM competitions influence the sub-discipline of career interest? Finally, is there a relationship between the number of competitions attended and the probability of interest in a STEM career? To find out, the researchers sent the Outreach Programs and Science Career Intentions survey to American students enrolled in English classes at institutions of higher learning. There were 15,847 returned surveys responses. Using logistic and multinomial regression models, they discovered that if a student had attended any STEM competition, there was a 5% greater likelihood she/he was in a STEM career at the end of high school. However, the survey's Sankey diagrams indicated that STEM competitions seemed to retain students already interested rather than bringing onboard new ones. Second, they found a strong relationship between participation and career interest when considering the field of competition and interest in a particular STEM's work category. Third, they noticed a more robust relationship when students competed in more than one competition. The authors, however, acknowledged that, although having controlled for many predictors of STEM career interest, this was a correlational study and did not clearly prove causation.

Melchior, Burack, Hoover, & Haque (2018) evaluated the impact of four FIRST programs. The longitudinal study tracked 1,273 students, comparing 822 FIRST team members and 451 students who did not attend over five years. Students were surveyed pre and post-program in their first year and then with annual follow-ups. The four-year impact report showed that FIRST participants continued to report greater average gains on STEM-related interest and attitudes (i.e. interest in STEM, involvement in STEM-related activities, STEM identity, STEM knowledge, and interest in STEM careers) than comparison students. In addition, despite enrolling in the program with a strong initial interest in STEM, FIRST participants were still "significantly more likely" to increase STEM interest and involvement over time. Moreover, FIRST programs continued to have an impact after participants left them, with alumni having a stronger interest in majoring in a STEM field, being more likely to choose an engineering course and more engaged in STEM activities in their first college year.

2.5.2 Cyber security competitions and interest

Even more pertinent to this research, some literature has investigated the relationship between cyber security skills competitions and interest; in other words, the extent to which these skills programme influence participants' cyber security interest. This literature is comprised of academic studies and the evaluation reports of some relevant national-level competitions (such as those described in section 2.2.2.1). One can identify two opposing sides: one that has found cyber security skills competitions increases interest in cyber security and one that is more sceptical.

On the one hand, some believe cyber security skills competitions can grow cyber security interest. For example, Werther, Zhivich, Leek and Zeldovich (2011) designed the MIT Lincoln Laboratory Capture-the-Flag Exercise to make these sorts of competitions more accessible. They assumed that participation in these events requires a priori knowledge and hands-on cyber security experience, which many computer science students do not possess. Hence, they created a competition that challenged the skills of participants but would also train those without prior knowledge through evening lectures and practical labs. In their post-competition survey, students reported having learnt much about practical cyber security. Moreover, when asked about their cyber security career interest, respondents said it increased by 1.1 point on a 10-point scale. However, the study was small, involving only 22 participants (Werther et al., 2011).

Cheung, Cohen, Lo, Elia and Carrillo-Marquez (2012) undertook their study on the same premise as Werther et al., stating that the effectiveness of competitions is limited because of the extremely high knowledge barrier. To lower this barrier, they designed a competition based on a hands-on learning methodology, including lectures, workshops and mock competitions. Although only nine students replied to the follow-up survey, their intervention increased student interest: students

showed more interest in taking further security courses, began inquiry about a cyber security career and started asking how to find an internship in this sector.

Bashir, Wee, Memon and Guo believed that “even though there have been many cybersecurity competitions over the last decade, it is still not clear whether competitors are interested in careers in cybersecurity” (2017, p. 155). So they surveyed 588 past attendees of the Cybersecurity Awareness Week, a competition organized by the New York University Tandon School of Engineering, which annually recruits 10,000 participants from all over the world. They found that 61% of participants were more persuaded to enter a career in cyber security after the competition, and that interest had a correlation of .24 (figure 5).

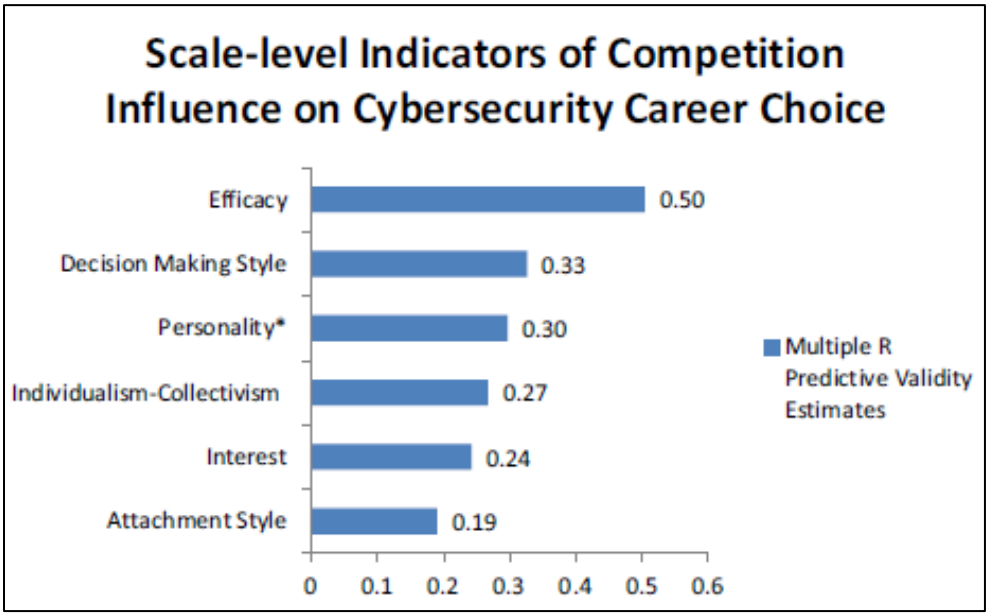

FIGURE 5 INDICATORS OF COMPETITION INFLUENCE (Bashir et al., 2017)

However, they acknowledged that one of the studies limitations was the use of retrospective self-report data, suggesting that future research should adopt a longitudinal approach with data points collected before and after the competition (Bashir et al., 2017). These findings were in line with previously found results from

the same research group, showing that the competition had made participants change their career plans in 22% of cases and “sort of” made them change their plans in 77% of cases (figure 6). When the competition had this influence, 86% of respondents had been more likely to pursue a cyber security career (Bashir, Lambert, Guo, Memon, & Halevi, 2015).

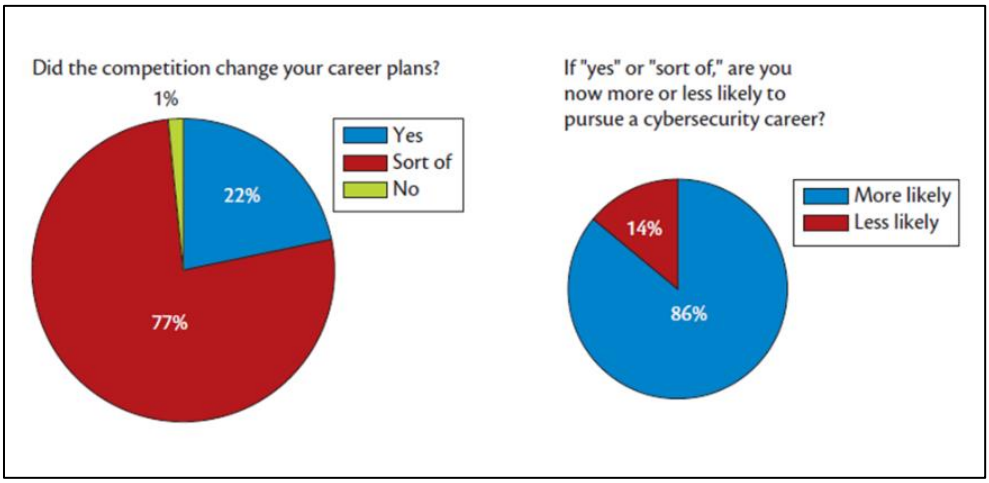

FIGURE 6 DID THE COMPETITION CHANGE YOUR CAREER PLAN? (Bashir et al., 2017)

In another study on cyber security workers’ perceptions, Wee, Bashir and Memon (2016) discovered that 58.4% of professionals currently employed in the sector thought their competition experiences influenced their decision to enter the field.

Dunn and Merkel (2018) sought to determine whether cyber security competitions increased interest in cyber security through a statistical analysis of CyberPatriot survey data. Results showed that interest in cyber security as an academic or employment career grew meaningfully across multiple dimensions, such as perception of career tasks, interest and awareness, and view of self. Furthermore, they found that those saying that they would have chosen a career in cyber security in the past are still planning to do so one year following the competition. Nonetheless, because of the lack of a control group, the study cannot make any causation claim, and the authors warned that it is unclear whether retrospective

questions had good explanatory power in determining how participants' interest changed throughout the competitions.

Finally, a recent impact report of the CyberTaipan pilot program presented promising results (AustCyber, 2019b). The pilot project consisted of online qualifying rounds, learning opportunities and the national finals. The report found:

- Participants to be twice as likely to pursue higher education in a cyber security field after the competition;
- There was a 490% increase in participants' awareness of cyber security roles;
- Participants to be almost three times more likely to pursue a career in cyber security after the event.

On the other hand, some researchers are more doubtful about the influence of cyber security competitions on interest.

Tobey et al. (2014) stressed that empirical studies on the effectiveness of cyber security competitions for increasing awareness, interest and engagement in cyber security careers are lacking. In their analysis of students participating in the National Cyber League, they found that competitions might be constraining the number of entrants in the field and discouraging the involvement of those with no prior experience. Hence, competitions might be better at further engaging those already committed to cyber security than those exploring it as a career option. Pusey, Gondree and Peterson (2016) reiterated this point, stating that the literature on competitions does not confirm that they attract and retain individuals who are not already involved in the sector.

Turner, Deemer, Tims, Corbett and Mhireì (2014) wanted to study the efficacy of an educational intervention program whose objective was to foster interest in cyber activity among high school students. The sample consisted of 60 students, most of whom were female (56%). They revealed that girls' perception of "cyber value" (intended as the perceived utility value of cyber activities) could increase if skills

needed for both STEM and liberal arts careers are integrated into an intervention. On the other hand, however, boys decreased their cyber value. As a possible explanation, they postulated that boys might have had too high expectations and when they faced difficulties during the programme, they may have devalued the importance of cyber science.

Finally, a critical piece of work was conducted by Campbell-Jack, Bickley and Lillis (2021a), who analysed the outcomes of the UK Cyber Discovery programme. This research is significant as it is, to the best of our knowledge, the only mixed-method study on the relationship between a *national* cyber security competition and various interest and career choice outcomes. In comparison, studies have generally investigated smaller scale competitions and are mainly quantitative. While the report acknowledged several limitations (i.e. absence of a counterfactual and a sample size not representative of the whole population), it presented the following findings:

- A higher number of respondents were very interested in studying (generic) computer science in the future (73%) than were very interested in studying cyber security (43%); similarly, 64% of respondents were very interested in a computer science career, compared to 43% who stated the same about cyber security;
- Students reported the programme contributed to increasing technical and computer science skills;
- Interest in computer science and cyber security did not change from pre to post-survey. One possible explanation respondents gave was that interest was already high before the competition. Qualitative information, however, suggested that the competition was very engaging for several students with a long-standing interest in computing and technology;
- There was no statistically significant change in interest in a computer science or cyber security career, which had remained high from pre to post programme; likewise, there was no statistically significant change in the

percentage of respondents who declared to be very interested in cyber security in the future;

- Most respondents said they were aware of further education or training opportunities such as cyber security degrees or apprenticeships; there was also a positive change in their understanding of different cyber security job roles and careers.

2.5.3 Summary and discussion

To sum up, this section reviewed the literature on skills competitions and interest. First, it presented the findings on the general literature on STEM competitions but then became more specific and showed results on cyber security competitions. There are three main takeaways:

1. The literature seems divided on the type of influence a skills competition might exert on participants' interest. Taking into account competitions' different aims and structures, one, therefore, should always assess competitions' outcomes rather than assuming them;
2. Many noted how entrance barriers to cyber security skills competitions are high due to the level of specific cyber security knowledge and skills required. The consequence could be that many students with no prior exposure to cyber security could be too demotivated even to enter them or face immediate failure in their first attempt, leading them to leave the programme and thus diminishing the chances of them entering the sector;
3. This literature has been particularly devoted to investigating interest in a career rather than interest in a subject/topic. This is not surprising as many of these competitions have been established in the hope to favour students' inflow into the technical workforce pipeline. However, it should not be assumed that interest in a topic and interest in a career go hand in hand. In fact, it may be possible for students to be interested in many subjects but to have narrower career interests or perhaps to have an interest in a topic but

have limited or no interests in a related career. This implies that research should be focused on understanding whether skills competitions influence interest in a topic as well as interest in a related career.

Besides these main takeaways, there are some essential methodological considerations that should be noted after reviewing the literature:

- No studies on cyber security competitions and interest had a suitable control group that could establish a solid counterfactual. Most of these studies were correlational and therefore could hardly make any causation claim;
- Studies generally featured small, sometimes unrepresentative, samples. For example, research on the UK Cyber Discovery Programme had a sample of 115 students, but the entire programme consisted of 35,941 signups (Campbell-Jack et al., 2021a);[11]
- Change in interest level is better assessed when a measurement is taken before and after the skills competition. As not all studies were able to do this, more evidence is needed on interest change following a before and after methodology;
- Mixed-methods studies are rare. Only Campbell-Jack et al. (2021a) have meaningfully attempted to merge quantitative and qualitative methods. However, it is critical to conduct mixed methods research to assess cyber security skills competitions fully. These are composite interventions, and quantitative-only studies are unlikely to grasp their full complexity in terms of dynamics at play and actors involved. Whereas quantitative analyses are needed to determine the extent to which a skills competition influences students' interest, qualitative data are equally important to discover how this occurs.

[11] The sample should have been of at least 381 students to be representative (95% C.L. and 5% margin of error).

2.6 Literature review summary and conclusions

This thesis is situated within a composite theoretical and policy picture, encompassing issues and topics belonging to various social science strands. This literature review has highlighted this complexity by building a framework that included labour economics, skills issues, policy interventions, competitions, and interest development. In order to reduce this complexity, this section puts the pieces of the puzzle together by summarising the relevant elements of the literature review. This is done with the aim of properly steering this research process in the following chapters, which will present the research questions and hypotheses (ch. 3) and the methodology (ch. 4).

Market failures occur because of several dynamics and factors, including technological change. The introduction of new technology creates skills mismatches when the labour market demands new skills that the supply side cannot offer in sufficient amounts. Skills shortages are a type of skills mismatch that ensue when there is a lack of qualified professionals applying for jobs. When such a shortfall occurs, some economists believe governments can correct the market through policy interventions.

The current lack of cyber security workers is compounded by issues found on both the demand and the supply side of the labour market. Among the issues localized within the supply side, one can observe the low number of students entering the cyber security sector. Governments have established national cyber security competitions (NCSSCs) to help solve this issue. NCSSCs are now widely popular and are possibly the most widespread policy worldwide to raise students' interest in cyber security. Governments hope that, by raising their interest, competitions' participants will then join the cyber security workforce. This hope seems well placed as interest is one of the drivers of career choice.

Some studies have investigated the influence of cyber security competitions on participants' interest, but the issue is far from being settled as research is divided

on the outcomes that these competitive events produce. Moreover, no literature has ever investigated how interest in cyber security is triggered and developed prior to a competition.

Against this background, this thesis aims to investigate the generation of cyber security interest among the participants of a national cyber security competition and discover the extent to which and how such intervention can influence such interest.

Studies on skills competitions (section 2.3), interest (2.4) and the relationship between skills competitions and interest (2.5) offer various pointers in the formulation of pertinent research questions, hypotheses and methods:

1. Past research indicated that skills competitions might have both benefits and drawbacks. Specifically, it is unclear whether and how skills competitions influence participants' interest as they usually imply high, initial knowledge barriers that could demotivate potential competitors even to try or face immediate failure in their first attempt. This may lead them to leave the programme and, thus, discourage them from entering the sector;
2. Notwithstanding the growing number of studies on skills competitions, one should be cautious in generalizing their findings. This is especially true in cyber security competitions as the literature highlighted their great variance in content and structure. For example, it would be hard to compare the results of a study investigating students' outcomes in a local cyber security competition taking place over two days with a study analysing the same dependent variable(s) but of a national competition occurring over several months. As the nature of such competitions differs, it is very likely that so too do their outcomes. Hence, research on a cyber security competition should detail the context in which it takes place as well as its objectives;
3. Some studies have attempted to link how the objectives of cyber security competitions can be reached through specific "means." For example, it has been highlighted that a well-designed, hands-on, and team-based cyber

security training programme is likely to lead to the development of cyber knowledge and skills among participants. Nonetheless, there is thinner evidence on how interest in cyber security as a topic and a career could be influenced in the context of a competition.

4. The concept of interest has been often studied in relation to interest in STEM subjects. Nevertheless, a thorough scientific inquiry into cyber security interest has never been conducted. Such inquiry could make an immediate contribution, especially if it could shed light on how cyber security interest is triggered and developed in the first place and understand the role that security competitions might have in influencing it.
5. The literature on STEM/cyber security competitions has been mainly focused on assessing variation in career interest. Fewer efforts have been dedicated to studying interest in cyber security as a topic and the relationship between this and interest in a career in the same sector. However, this should be further investigated as it could be possible for a student to be interested in a topic, but not necessarily in a career in cyber security sector, something that would have important implications for a programme designed to increase both.
6. There are no established and universally accepted methods to measure interest because of the variety of disciplines, research aims and methods that have been involved in the study of this concept. Nonetheless, research on interest does not occur in an intellectual vacuum and could be supported by previous findings and research methodologies that are in line with its aims. Having said this, the literature suggested that a study using surveys with multiple items and other sources of information such as interviews is more likely to produce solid evidence.
7. In light of the specific research on cyber security competitions and interest, there are several critical methodological considerations that a thesis on this subject should be aware of, namely:
    - No past studies assembled and used a control group and were, therefore, able to establish a suitable counterfactual;

- Past research has usually featured small and often unrepresentative samples of the study population. As even randomization is challenging (if not impossible) when investigating national cyber security competitions, their results should be taken with caution;
- Changes in cyber security interest are better assessed when measurements are taken before and after a skills competition rather than only after. As it will be further explored in the methodology, a before-and-after research design reinforces any direct causation claim;
- Few studies used mixed-methods to reach their research objectives. Further research should fill this gap and collect qualitative evidence on cyber security skills competitions. These are complex programs whose dynamics could be fully appreciated with the addition of qualitative data. Moreover, this method of data collection and analysis would directly tackle one of the current major knowledge gaps regarding cyber security skills competitions, namely understanding which factors (i.e. “how”) contribute to shaping interest during the programme.

3. Research questions and hypotheses

This chapter introduces the research questions and the hypotheses of this thesis, which are guided by both the problem definition (ch. 1) and the literature review (ch. 2).

Research questions:

This research project seeks to answer two main research questions:

1. How do participants develop an interest in cyber security before attending a NCSSC? What factors specific to cyber security may trigger the development of such interest?
2. Do NCSSCs influence participants' interest in cyber security as a topic and as a career? What factors contribute the most to influence it?

By addressing these two questions, this thesis seeks to discuss the role of national competitions as a public policy to mitigate the skills shortage.

Research questions and hypotheses

1) How do participants develop an interest in cyber security before attending a NCSSC? What factors specific to cyber security may trigger the development of such specific interest?

This research question analyses how competition participants became interested in cyber security before signing up for it, which is a question that has not been yet investigated in the current literature. Answering this question is set to make an immediate contribution as it provides content-specificity (i.e. cyber security) to interest development theory. Cyber security may become a valuable case study, from which wider lessons can be drawn and applied to the general literature on interest.

The hypothesis is that NCSSC participants would typically have already developed a strong interest in cyber security before the beginning of the programme or, to use interest research vocabulary, a *well-developed individual interest*. They would have done so mainly because NCSSCs are content-specific competitions (cyber security vis-à-vis more generic computer science programming events), requiring exact high-level knowledge and skills due to being held at the national level, which increases their competitiveness.

Participants should become interested in cyber security through various triggers. One hypothesis is that participants would develop interest on their own by seeking relevant information. I would also expect to be triggers cyber security specific activities such as formal high school or university coursework and prior participation in local cyber security skills competitions, but not a national one. In fact, one hypothesis is that a NCSSC is unable to generate cyber security interest among its participants as they are likely to have developed a well-rounded cyber security interest prior to it in order to be able to compete at the national level. A final hypothesis is that key figures such as parents, teachers, and peers, who are often central in creating the learning environment, designing the tasks, and providing information, will strongly influence participants' interest.

2) Do NCSSCs influence participants' interest in cyber security as a topic and as a career? What factors contribute the most to influence it?

This research question is central to investigating the relationship between skills competition and interest. The literature is divided on whether skills competitions should be incorporated in educational settings and the extent to which they influence interest; moreover, it is silent on the factors (i.e. "how") that supposedly influence interest. Feeding this debate is important for policymaking as well, as NCSSCs are among the most widely implemented policies to mitigate the lack of cyber security professionals. Hence, knowing whether they reach their intended objective is relevant to assessing whether countries are on the right track in dealing with the problem.

This thesis will differentiate between interest in cyber security as a topic and interest in cyber security as a career in order to study the extent to which and how a national cyber security skills competition influences the interest of participants. It does so mainly because the literature review found that the relationship between interest development and vocational interest needs to be further unpacked. One hypothesis is that NCSSC participants do not differentiate between the two, namely their interest in cyber security as a topic is equal to their interest in cyber security as a career, and this interest will be influenced (or not) by a NCSSC to the same extent. The logic is that, because students entering the competition are likely to have a *well-developed individual* interest in cyber security, they are also likely to consider it their first career option.

On the relationship between NCSSCs and interest, the main hypothesis is that NCSSCs either do not affect or decrease participants' interest in cyber security. The logic of this hypothesis is as follows. Although cyber security competitions might attract individuals from different backgrounds and with varying levels of commitment to the field, only a few participants make the most out of them because of the high-level entry barriers (Cheung et al., 2012; Tobey et al., 2014; Werther et al., 2011), especially in national events. These participants are those who enter the programme and enjoy a prolonged experience with like-minded and equally skilled peers. To enter a competitive event such as a NCSSC, these individuals have likely honed their skills and already developed a strong interest and commitment to the field before entering the programme. Once they enter it, though, the competition is unlikely to affect how they feel about cyber security as their interest was already high before commencing it. Hence, in more formal terms: the cyber security interest of participants admitted to the latter stages of the competition (the so-called treatment group in this research, see chapter 4) is kept constant, meaning it does not significantly increase or decrease, as a result of participation in the cyber security competition. On the other side, the participants who would need to have their cyber security interest influenced are unlikely to access the competition because of the high-level admission criteria, which only a small group of individuals can manage to meet. Their inability to enter the skills

programme is likely to make them give up on cyber security as they will think that cyber security is not a right fit for them if they cannot enter the competition. In the end, as the nature of NCSSC is competitive and large-scale, it is the participants that should be exploring cyber security who are the least likely to become more interested in the sector. Hence, in more formal terms: the cyber security interest of non-admitted participants (the control group, see chapter 4) will be decreased by the cyber security competition.

The second part of this question *("What factors contribute the most to influence their interest?"*) is as important as the first part because it seeks to identify the key aspects and explain the mechanisms shaping participants' interest. This is important as the literature has not connected the "objectives" of cyber security competitions with their "means" yet. Answering this question allows an in-depth exploration of NCSSCs and shed light on the findings of the previous question. Furthermore, by researching how individuals belonging to different groups (i.e. control vs treatment groups) experience the competition, this research could produce more prescriptive statements on improving challenges. Following the logic of the hypotheses above, the admission process should be an important determinant of how cyber security skills competitions influence participants' interest. More specifically, as the admission process is likely to select a small portion of students who are already highly interested and skilled, it may discourage non-admitted students from further pursuing cyber security. On the other hand, the literature found the training-skills challenge combo and career-awareness activities to be important factors. However, it is unclear what they can achieve in affecting interest. Regardless, as the admitted participants will likely have already developed solid cyber security interest, skills and knowledge, the cyber security training is unlikely to have a significant influence.

By answering these two questions, this thesis aims to discuss the role of national competitions as a public policy to mitigate the skills shortage, which can be

summarized with the following question: are NCSSCs an effective policy to tackle the shortfall of cyber security professionals in the labour market?

This question is different from the previous two. While this research will collect data to answer the previous two questions, this final “question” on NCSSCs as an instrument to tackle the shortage will not rely on newly generated data. Instead, it will rely on previously collected information to have a broader discussion on the role of skills competitions. This is done to have a final and holistic assessment of competitions (in chapter 9), integrating the data collected for the first two questions.

The overall expectation is that NCSSCs are not an effective policy tool to address the shortfall of cyber security professionals. Because of their high-level entry requirements and competitive nature, NCSSCs are unable to generate interest in the first place; instead, they attract participants that are already highly skilled and motivated to pursue a cyber security career, making it more difficult for newcomers to access these events and explore the field. Because of this, an NCSSC is unlikely to increase the number of individuals interested in cyber security who might end up pursuing a career in the sector.

4. Methodology

This chapter presents the methodology of this thesis, which is based on a before-and-after research design; it collects data from CCIT participants belonging to non-randomized groups and uses mixed methods.

This chapter is organised as follows:

- section 4.1 covers the operationalisation of this research and explains the context in which it took place. It also clarifies why the Italian national cyber security skills competition (NCSSC) was selected as the case study of this research;
- section 4.2 briefly describes the principal elements and main phases of the Italian NCSSC and how Covid-19 impacted it;
- section 4.3 justifies and provides a bird's eye view of the research design and explains how the operational setup of the Italian NCSSC influenced it;
- section 4.4 details the mix-methods approach that was used to collect and analyse data;
- section 4.5 gives an overview of the ethical elements that this thesis had to consider before beginning the data collection process;
- section 4.6 provides a summary of this chapter.

4.1 Operationalisation: definition, context and choice of case study

This section defines NCSSCs and provides the overall European context in which they occur. It also explains the criteria behind the choice of the Italian NCSSC as a suitable case study. This section precedes section 4.3 on the research design as this thesis' methodology was strongly shaped by the organization and implementation of the skills programme.

For the purpose of this research project, an NCSSC is defined as national-level cyber security “interactive, scenario-based event or exercise, in person or virtual, where individuals or teams engage in cybersecurity activities including methods, practices, strategy, policy and ethics” (NIST, 2018). In addition, cyber security is identified as any topic within the top-level knowledge areas of the Cyber Security Body Of Knowledge (Rashid et al., 2018).

To further limit the scope, this research considered only those NCSSCs organised by those countries whose national teams attend the European Cyber Security Challenge (ECSC). The ECSC is the pan-European cyber security competition organized and coordinated by the European Union Network and Information Security Agency (ENISA),[12] where national teams congregate and compete in domains such as web security, mobile security, crypto puzzles, reverse engineering, and forensics. The popularity of the ECSC has grown exponentially in recent years. The first edition of the ECSC took place in Austria in 2014, where 30 participants from only three national teams attended (ENISA, 2017). Five years later, 20 national teams and 200 competitors from all over Europe flew to Romania for the 2019 ECSC edition (ENISA, 2019). According to ENISA, the ECSC is based on the premise that the "growing need for IT security professionals is widely acknowledged worldwide" and that many countries in the EU have organised cyber security competitions "with a clear aim to find new and young cyber talents and encourage young people to pursue a career in cyber security" and "to help mitigate this shortage of skills" (ENISA, 2019).

There are hundreds, if not thousands, of cyber security competitions and skills challenges worldwide. However, this research focused only on national programs leading to the ECSC because these competitions usually receive support from their countries and EU institutions, and thus can be considered public policy interventions.

[12] The EU Cybersecurity Agency.

The literature review found that cyber security skills competitions come in all sorts of configurations and shapes (Conti et al., 2011; De Zan & Yamin, 2021; van Rensburg & Baker, 2021). As designing a study that includes two or more competitions with different planning and organisational structures would have been methodologically challenging, let alone accessing data, this research studied only one NCSSC. The chosen case study was the Italian national cyber security challenge, the CyberChallenge.IT (CCIT), which is the NCSSC in Europe that trains the largest number of participants for at least three months (figure 7) (De Zan & Yamin, 2021). The rationale behind this choice was that the influence of the CCIT is likely to be more pronounced than the influence of any other competition with a shorter duration and thus better observable.

FIGURE 7 NUMBER OF TRAINEES AND LENGTH OF TRAINING IN NCSSCS IN EUROPE

4.2 The CyberChallenge.IT and the impact of Covid-19

The Italian CCIT is a "training opportunity" for high school and undergraduate students whose goal is to identify, attract, recruit and place the next generation of

IT security professionals. The overall aim is to "significantly reduce the current shortage of the IT workforce" and make students' skills available to the country. According to the organisers, attending can be a first step towards a career in cybersecurity, and the program is part of the national cyber security strategy to improve the Italian cyber security workforce (CyberChallenge.IT, 2019; Porro, 2019). In line with other NCSSCs worldwide, CCIT's objectives are to:

- ***stimulate interest*** *in technical-scientific subjects and, in particular, in information technology topics* (emphasis added)*;*
- *present the professional opportunities offered by the training courses on information security* (emphasis added)*;*
- put young people in direct contact with companies;
- identify young cyber talent, contributing to their orientation and professional training;
- to search for and select more female talent and high school students (CINI Cybersecurity National Lab, 2019).

Students can sign up to the CCIT if they are between 16-23 years old, fluent in the C or C++ programming languages and understand English. No prior cyber security knowledge is required, and attendance is free of charge.

Students sign up online and perform an online pre-test based on logic and programming skills to enter the competition. Then, the best performers are invited to an on-site admission test at one of the participating local universities. The on-site test consists of a morning and an afternoon test based on logic and programming quizzes. The 20 students with the highest score from each local university are selected to attend the CCIT. Once the programme starts, the selected students undergo a 3-month cyber security training, at the end of which they compete in a local skills challenge. Finally, the six best students from each university are invited to attend the final national skills challenge (CyberChallenge.IT, 2019).

The outbreak of Covid-19 inevitably shaped the timeline, structure and delivery of the 2020 CCIT edition. The paragraphs below present a brief chronology to understand the extent to which the health emergency impacted the CCIT and this research:

- February 19: the CCIT announced the end of the admission process.
- February 24: the Civil Protection Department, the Italian institution coordinating crisis management operations, reported that 229 people had been infected with Covid-19 in the first televised press conference on the topic (Dipartimento della Protezione Civile, 2020).
- March 6*:* the CCIT confirmed the continuation of its training programme in an online format in light of the unfolding health emergency.
- March 9*:* In the night between March 9 and 10, the Italian government declared a total national lockdown. Citizens were told to avoid unnecessary travel and stay at home (ANSA, 2020b); stricter measures followed three days later, when the government ordered all non-essential shops to close (ANSA, 2020a).
- April 28*:* the CINI's Cybersecurity National Lab, the entity organizing the CCIT, announced the expansion of the CCIT program with a new component, the OpenCyberChallenge.IT (OCCIT). With the OCCIT, the CNL allowed access to cyber security learning material to the students who had taken part in the admission test but had not been admitted to the training (CINI Cybersecurity National Lab, 2020d).
- June 3*:* ENISA announced the cancellation of the 2021 edition of the European Cyber Security Challenge "due to the worldwide pandemic and the lack of visibility regarding its evolution" (ENISA, 2020).
- June 8*:* the CCIT local skills challenges took place at each university (in an online format). Six winners from each local university were selected to compete in the national skills challenge (CINI Cybersecurity National Lab, 2020b).

- August 4: the CINI Cybersecurity National Lab announced that the final national competition would take place online on October 1 and 2 – instead of July 9 and 10 as previously planned – due to the international health crisis (CINI Cybersecurity National Lab, 2020a).
- October 1-2: The national skills challenge took place, consisting of an online attack-defence skills competition and a presentation to a jury of experts (CINI Cybersecurity National Lab, 2020c).

The final timeline of the 2020 CCIT edition looked as follows:

FIGURE 8 PHASES OF THE 2020 CCIT EDITION. SOURCE: *(CYBERCHALLENGE.IT, 2019)*

The Covid-19 crisis had three important consequences on the CCIT and subsequently on this research:

1) The pandemic delayed by 12 weeks the beginning of the second data collection phase, which started on October 5 instead of July 13. Because of difficulties in obtaining an adequate number of replies in the second survey, the second round of data collection ended on December 18. Therefore, the health emergency's main implication was the delay of the data collection process, which reduced the overall time to process and analyse the data.

Notwithstanding the unwelcomed delay, this postponement had at least two unintended positive consequences. The first is that this delay increased the time between the first and the second data collection, which allowed a deeper examination of the themes emerging from the first round of data. These data yielded insightful results, which were deemed interesting enough to be further explored in the second data collection.

The second positive consequence was that the survey was launched in October, well after participants started the new academic year. This meant that some students made (and could report on) their education and career choices, namely whether they graduated from high school and enrolled in a bachelor's degree or enrolled in a master's degree or started employment. This led to the possibility of knowing more about whether the CCIT had an influence beyond cyber security interest and whether it concretely induced participants to choose a different educational or career trajectory. These results provided a more rounded understanding of the CCIT influence and are the main thrust of chapter 8.

2) As schools and universities were closed after the March national lockdown, Covid-19 forced the CCIT to deliver the training online rather than the foreseen in-person/on-site format. The new format did not cause any change in either the research design or the data collection procedures of this study, but it altered the programme. The question is whether this changed the CCIT to the extent of invalidating the research results. To ascertain if this was the case, I directly asked participants who underwent the training to describe the impact of Covid-19 on their CCIT experience. As chapter 9 will show, several interviewees lamented that the learning experience had not been as engaging as it could have been if it had occurred face-to-face. Some participants also felt that the online delivery had made the experience slightly impersonal as they were unable to forge closer relationships with their colleagues. However, it can be argued that the CCIT was not altered to the extent that the whole program was impaired. In fact, the content, tools and structure of the cyber security training did not change. According to the interviewees, the training and the local and national challenges were enjoyable

and were considered a success; the online training did not prevent students from finding lessons entertaining or creating deeper relations with their instructors and programme fellows. Hence, while this thesis duly noted all the elements that potentially changed the nature of the CCIT, it can be maintained that the consequences of Covid-19 were not so vast to skew the outcomes of the CCIT and consequently this research.

3) The pandemic allowed CCIT organizers to expand the programme to the students initially left out with the new OpenCyberChallenge.IT (OCCIT) initiative. The objective of the OCCIT was twofold: to permit students to increase their level of cyber security knowledge and to maintain interest in the CCIT project, with a view to encourage them to reattempt admission in 2021. Students accessing the OCCIT platform could access lectures, skills challenges, crash courses and additional teaching material for each weak of the 12-week training period. The students who followed 75% of lectures and completed 90% of challenges were awarded a certificate of attendance (CyberChallenge.IT, 2020). This meant that students who were in the control group and who were not originally supposed to receive any training instead might have opted to receive some. An important consideration is to understand whether the OCCIT was similar to the "conventional" CCIT and verify the potential claim that people doing the OCCIT programme underwent a similar "treatment" to those doing the conventional CCIT, so that the influence of the regular CCIT could not be distinguished from the OCCIT. According to the organizers, however, the OCCIT programme did not come close to the learning experience offered by the CCIT. CCIT students enjoyed live lectures and weekly skills challenges in the practical labs; they could also put into practice what they learned in the local and national challenges. On the other hand, OCCIT students could only access pre-recorded lectures on a limited number of topics and only on-demand cyber security skills challenges. Thus, the nature of the two programmes was so different that it could hardly be argued that the OCCIT was similar to the CCIT. While the introduction of the new programme did not change the major design elements of this research, it was evident that the OCCIT introduced novelties to take into account in the data collection. Therefore,

the second survey included a question to record the presence of students who enrolled in the OCCIT, but did not complete it, and those instead who enrolled and concluded it. Similarly, some study participants took part in the OCCIT and discussed how this changed their views on cyber security. Overall, this gave additional insights on how a programme that was different from the conventional CCIT could influence cyber security interest among participants.

To conclude, it can be contended that the main issue stemming from the Covid-19 emergency crisis was the postponement of the second data collection phase and the overall delay of the research process. Fortunately, however, it did not cause any change to the research design and data collection procedures. Finally, new interesting elements brought in by the OCCIT programme were detected by the data collection and investigated further in the analysis.

4.3 Research design and methods

4.3.1 Research design

This research had two main goals: 1) to understand how participants developed their cyber security interest before the CCIT; 2) to determine the influence of the CCIT on participants' cyber security interest and how this occurred. To accomplish these goals, the research design features some elements of evaluation research, which has been applied to the education arena for over half a century (Nevo, 2006). In this field, one of the purposes of the research design is to exploit an intervention’s intrinsic characteristics to estimate the best possible counterfactual and make more substantial causal claims (Owen et al., 2011). The structure of the CCIT made it possible to model this inquiry according to a before and after design using non-randomized groups for comparison purposes.

A before and after design measures the dependent variable (i.e. cyber security interest) before and after a programme (i.e. the CCIT) to understand how the intervention influenced it. A study of this kind is significantly strengthened when it

relies on data from before and after, as this permits a more rigorous assessment (White & Raitzer, 2017). The literature review in chapter 2 noted that not many studies have relied on before and after designs, decreasing their strength. In the case of this research, measurements of cyber security interest were taken before the CCIT commenced in February 2020 and in October 2020, at the end of the programme.

The difference between true experiments and quasi-experiments is useful in understanding how, why and "from where" this research collected its data. In true experiments, the researcher creates treatment and control groups according to a randomization process and makes sure those groups are comparable to the best extent possible. In quasi-experiments, instead, the setting of a programme determines the group receiving the treatment and the group that does not, meaning that treatment and control groups are not established according to a randomization process (Bryman, 2015). This research takes inspiration from quasi-experimental designs by collecting data from individuals belonging to "comparisons groups" that the CCIT created through its admission process. The CCIT's admission process established two different groups:

- a "treatment group" (TG), which received the treatment: the students who passed the admission test and underwent the three-month cyber security training followed by the local and national skills challenges (i.e. the "treatment");
- a "control group" (CG), which did not receive the treatment: the students who sat the onsite admission tests but were not admitted to the programme.

This is an important step forward in a study of cyber security competitions. The literature review noted that previous studies had not established strong counterfactuals by creating (or exploiting) effective comparisons groups, which limited their causation claims. While the lack of randomization which characterized the allocation into treatment and control groups also restricts the causation claims that this research can offer, this study goes in the right methodological direction by

comparing a group of individuals who underwent the CCIT training with a group of individuals who did not.

4.3.2 Research methods

The following sections present how data were collected and analysed using mixed-methods. The quantitative component of this research sought to understand the extent to which the CCIT influenced participants' cyber security interest, utilizing surveys as an instrument of data collection and analysis. The qualitative component aimed to understand the process of cyber security interest development and how the CCIT was enacted, using interviews with participants as its primary tool.

This mixed-method approach was "convergent" (figure 9) (Creswell & Creswell, 2017), whereby quantitative and qualitative data were merged and integrated to provide a comprehensive understanding of the phenomenon under investigation, with a view to interpret the results holistically.Both quantitative and qualitative data were collected simultaneously, before the start of the CCIT programme and at the end.

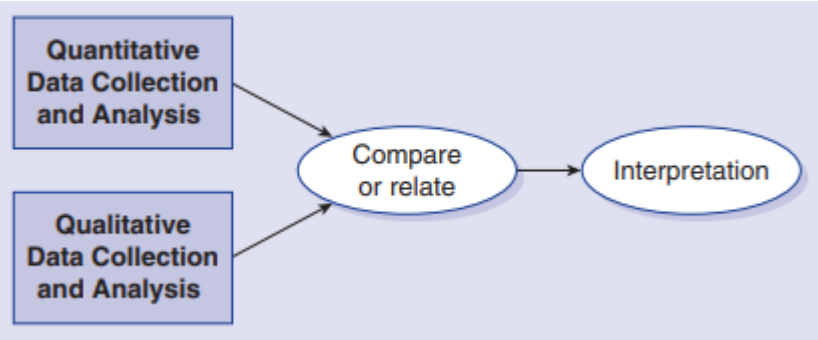

FIGURE 9 THE CONVERGENT PARALLEL DESIGN. SOURCE: *(CRESWELL & CRESWELL, 2017)*

This section is further divided into two subsections: 3.3.1 presents how quantitative data were collected and analysed, while 3.3.2 does the same for the qualitative component.

4.3.2.1 Quantitative component

The quantitative part of this research had the objective to discover the extent to which the CCIT exerted an influence over participants' cyber security interest. This section explains how data were collected and analysed and is organised as follows:

- 4.3.2.1.1 explains how the survey instrument was formulated;
- 4.3.2.1.2 describes the data collection procedures;
- 4.3.2.1.3 presents how the quantitative data analysis was performed.

4.3.2.1.1 OUTCOME VARIABLE MEASUREMENT AND SURVEY INSTRUMENT

Cyber security interest is the main dependent variable of this thesis as well as the outcome that the CCIT is expected to influence. A focus on outcomes is usually associated with quantitative measurement, as a study measuring them is helpful to the extent that it can estimate a programme's progress towards the intended objectives (Brisolara, 2018).

Drawing from the literature on interest (K. Ann Renninger & Hidi, 2020), this research defines cyber security interest as: a cognitive and motivational variable that describes 1) engagement, or participation, with cyber security content and also 2) the motivation to continue to seek opportunities to engage with cyber security content: seeking information, posing questions, and tackling a challenge. Vocational interest reflects "the degree to which individuals prefer certain career choices or activities/behaviors which may be common for various positions" (Schermer, 2016).

As several scientific studies have already examined interest, this research relied on existing survey instruments and items to measure it rather than developing a new one. The instruments reviewed were:

- Test of Science Related Attitude (Fraser, 1981);
- Utrecht Work Engagement Scale (Schaufeli, Bakker, & Salanova, 2006);
- The Career Interest Questionnaire and the STEM Semantics Survey (Tyler-Wood, Knezek, & Christensen, 2010);
- Persistence Research in Science and Engineering (Dabney et al., 2012);
- Aspires 2 Year 13 Survey KCL Questionnaire (DeWitt et al., 2013);
- The Relevance of Science Education (University of Oslo, n.d.);
- The STEM Career Interest Survey (Kier, Blanchard, Osborne, & Albert, 2014);
- Interest & Recruitment in Science Q Master Version (Henriksen, Dillon, & Ryder, 2015);
- "Questions to determine "will enter"/"won't enter" groups" (Bashir et al., 2017);
- CyberPatriot Student Alumni Survey and CyberPatriot VI Post-Season Competitor Survey (Dunn & Merkle, 2018);
- YISTEM A – Items on career interest (Ali, Talib, Surif, Ibrahim, & Abdullah, 2018);
- For Inspiration & Recognition of Science & Technology survey (Center for Youth and Communities, 2019).

These instruments were reviewed according to relevance and empirical standards of measurement validity (Morrow, Mood, Disch, & Kang, 2016). When closely inspected, some of the items used in previous studies did not seem to be directly relevant in terms of face and content validity and were therefore dismissed.[13] Moreover, as most previous instruments measured generic STEM interest, some

[13] For example, the Utrecht Work Engagement Scale (Schaufeli et al., 2006) used by Tobey et al. (Tobey et al., 2014) seems to be an instrument more suitable to study engagement on the work place (as the appellation of the survey would suggest) rather than career interest.

of the indicators/items had to be adapted to reflect the specificity of this research. Finally, as this study was not an integral part of the CCIT, but rather a “side” project that organizers agreed to, and since attrition rate was a concern, after collecting approximately 25 items representing the construct of cyber security interest,[14] they were reduced to 15.

The first iteration of the survey was tested in a small pilot study. The pilot phase took place between January and February 2020 and involved students who had participated in the 2019 CCIT edition. These participants were listed on the CCIT website and were recruited through social media. Five students were invited and were asked to complete the online survey as well as undertake an interview. They were rewarded with a €10 voucher for their time. The pilot was beneficial to improve the questionnaire and finalise the first "before" survey, which was sent out at the end of February 2020. The second "after" survey questionnaire, sent at the end of the competition in October 2020, had some questions added to validate some of the results and emerging themes of the first (qualitative) data collection round.

Both surveys were first redacted in English and later translated into Italian to ensure CCIT participants effectively understood them. They can be found in annex II for further examination.

The platform used to design and distribute the surveys was Jisc Online Surveys,[15] which was chosen following an informative session with the University's IT Support Centre. Jisc was chosen because of its flexibility as well as compliance with the EU General Data Protection Regulation, which was an essential pre-requisite since the survey collected data from EU citizens.

[14] Mainly from (Center for Youth and Communities, 2019; Fraser, 1981; Kier, Blanchard, Osborne, & Albert, 2014; Tyler-Wood, Knezek, & Christensen, 2010).
[15] https://www.jisc.ac.uk/

4.3.2.1.2 DATA COLLECTION PROCEDURES

The first pre-survey was sent on February 28 and was closed on March 29. The survey received a total of 965 answers, which decreased to 895 after data cleaning, out of 4,454 individuals who signed up online. Therefore, the survey had a response rate of 20,1%.

TABLE 5 PRE-SURVEY RESPONSE RATE

Before survey	
Population size	4,454
Responses	897
Response rate	20,1%
Sample size needed	354 (C.L. 95%) 580 (C.L. 99%)

The second post-survey was sent on October 7 and was closed on December 18. The survey received 448 answers, which decreased to 390 after checking for duplicates and bogus answers, thus with a response rate of 9%.

Receiving an adequate number of responses in the second survey was a challenge, which became immediately evident when the survey was launched: on the first day, the second survey received only 130 replies, compared to the pre-survey, which received 576. In an attempt to encourage participation, I secured extra funding to award more vouchers. Furthermore, I asked CCIT organisers to send three reminders, two to the whole population (participants who signed up online) and one only to the relevant control and treatment groups. As these reminders had limited effects, two more personalised reminders were sent to the control and treatment groups. The survey was closed on December 18. In total, the research granted 178 vouchers worth €10 – for a total of €1780 (£1,650) – to the participants who completed both surveys.

TABLE 6 POST-SURVEY RESPONSE RATE

After survey	
Population size	4,454
Responses received	448
Responses after data cleaning	390
Response rate	9%
Sample size needed	**354 (C.L 95%)** 580 (C.L. 99%)

Despite receiving 390 responses, the second survey did not obtain enough replies from the students belonging to control and treatment groups to perform a statistically sound difference-in-difference (DiD) analysis, which was the chosen statistical framework of the quantitative component of this thesis.

Issues with response rates and sample sizes have been beleaguering survey research for a while and are not unique to this project. For example, Boyle and colleagues found that response rates on major surveys such as US federal ones have been declining from 70% to 40% or less over the last 20 years (Boyle et al., 2021). An example from a study in the same field is perhaps even more compelling. Campbell-Jack et al. sought to analyse changes in cyber security interest among participants of the UK Cyber Discovery programme (2021a). They surveyed a population of 35,941 students and received 115 responses, meaning a response rate of 0.003%. This result is further put in perspective when one considers that the study was commissioned by the organization implementing Cyber Discovery[16] and was supported by the Department for Digital, Culture, Media & Sport of the UK Government, the main sponsor of Cyber Discovery.

[16] The SANS institute, one of the leading providers of cyber security training in the world.

The following section explains why the DiD analysis had been chosen as the main framework for the statistical analysis and why the response rate of the second survey did not allow to have a statistically sound DiD; it also explains how the collected quantitative data were used instead in the context of this research.

4.3.2.1.3 QUANTITATIVE DATA ANALYSIS

As stated above, the allocation of participants into treatment and control groups indirectly undertaken by the CCIT admission process greatly influenced how this research collected and analysed quantitative data. Generally speaking, when allocation into comparison groups is not randomized, it is essential to consider how the allocation was undertaken, how this shaped the non-equivalence of the two groups and what kind of information should be gathered which can be helpful for the analysis (Owen et al., 2011).

In the CCIT, control and treatment groups were determined by the February on-site admission test, which suggested using a Regression Discontinuity Design (RDD). However, using this design was impossible for various reasons, as explained in annexe III. Thus, because the admission test assignment method was neither fully randomised as in a randomised control trial, nor fully deterministic as in an RDD, a DiD offered a more appropriate statistical framework.

A DiD is the difference between the outcomes of two groups over time, and it is based on subtracting the control group's changes from baseline (before the CCIT) to end line (after the CCIT) from the treatment group's changes from baseline to end line. The DiD removes differences at the baseline as these differences have not been generated by a programme like the CCIT (White & Raitzer, 2017). More formally, it can be expressed as below (figure 10):

$$DiD = (Y^1E - Y^1B) - (Y^0E - Y^0B)$$

Where:

- Y^1E: value of cyber security interest **after** the intervention in the *treatment group (TG)*;
- Y^1B: value of cyber security interest **before** the intervention in the *TG*;
- Y^0E: value of cyber security interest **after** the intervention in the *control group (CG);*
- Y^0B: value of cyber security interest **before** the intervention in the *CG*.

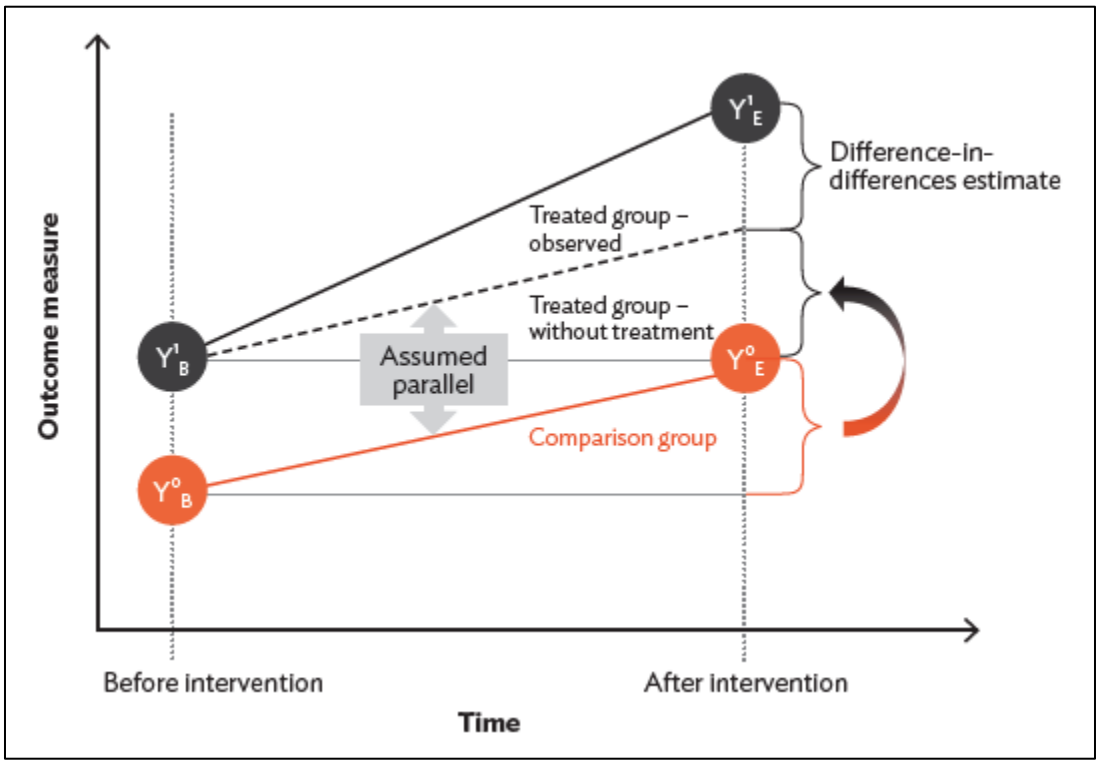

FIGURE 10 ILLUSTRATION OF DIFFERENCE-IN-DIFFERENCE. SOURCE: (White & Raitzer, 2017)

For the reasons above, this method would have required an appropriate number of responses in both the pre and post-surveys. Because the DiD analysis aims to

compare groups within the overall population, it would have required an adequate number of responses specifically from the control and treatment groups to understand changes in cyber security interest from pre to post. While the first survey successfully collected enough data, the second did not. Table 7 (below) shows the number of responses received by each group and per survey, as well as the required sample size to operate a solid DiD analysis.

TABLE 7 RESULTS TO PRE AND POST-SURVEYS

	Pre-test online	Morning test	Afternoon test	Admitted to CCIT	Total
Population size	891	421	888	560	2,760[17]
N 1st survey responses	150	136	295	314	895
N 2nd survey	66	55	143[18]	126	390
N students who replied to both surveys	**25**	**32**	**86**	**78**	221
Sample size required	**269 (95%)** 382 (99%)	**202 (95%)** 259 (99%)	**285 (95%)** 415 (99%)	**229 (95%)** 305 (99%)	

Hence, because the admission process did not create control and treatment groups based on randomization (with the consequence of a significant collinearity and highly skewed data, which emerged from a preliminary analysis) and the

[17] Number of students who signed up and performed at least the online pre-test. Therefore, this figure does not include the individuals who signed up to the CCIT but did not perform the pre-online test (N= 1694)

[18] This figure includes those were admitted to the CCIT but dropped out of the training programme. Even though these individuals had been admitted to the CCIT, for the purpose of the analysis they did not receive the treatment.

inability to have an adequate sample size for the comparison groups, it was decided to employ the data generated by the surveys for descriptive purposes, highlighting emerging themes and trends in conjunction with the qualitative data. This seemed a good compromise as descriptive statistics is still useful in describing the main features of the data and forming “the basis of virtually every quantitative analysis of data” (Trochim, 2021).

Because of these issues, the qualitative component of this research assumed an even more prominent role. Hence, the following section explains the rationale of the qualitative data collection and analysis and how it helped achieve this thesis's objectives.

4.3.2.2 Qualitative component

The qualitative component sought to discover how CCIT participants developed an interest in cyber security before taking part in the skills programme and how the CCIT influenced this interest. This was done by conducting one-on-one Skype interviews with CCIT participants. Interviews were chosen as the most suitable data collection instrument as they are useful in describing participants' experiences and self-understanding, with the possibility to elaborate on their perspectives of their lived world (Kvale, 2007b). Therefore, interviews were used to gauge how participants interest in cyber security was formed, their competition experience and how it influenced their perspectives on cyber security.

This section is comprised of the following subsections:

- 4.3.2.2.1 describes the interview sampling strategy based on the overall research design;
- 4.3.2.2.2 presents how the initial interview script was drafted and how the pilot study improved it;
- 4.3.2.2.3 explains the recruitment process and the overall data collection procedures;
- 4.3.2.2.4 details how qualitative data were analysed.

4.3.2.2.1 SAMPLING STRATEGY

This research followed a purposive sampling strategy, and therefore it identified and interviewed individuals who were likely to elucidate important elements of the research questions. Although the sample size did not reflect any concern related to the statistical representation of the population, it addressed diversity and included all the relevant elements of the research design in line with Owen et al. (2011).

Following the overall pre and post design approach, I conducted interviews with CCIT participants in the control and treatment groups before the CCIT and at the end. The literature calls this "before and after case study design," which are particularly useful "for understanding specific contexts where the how and why of behaviour are important, the context impacts the behaviour, and there are pivotal events impacting people" (McDonald, 2010, p. 52). Although this method has been employed in other fields,[19] it has never been employed in studying skills competitions and interest development.

More specifically, I interviewed participants from both the control group (CG) and the treatment group (TG). Listening to students belonging to both groups helped obtain a holistic understanding of how computer science students attending a national skills competition might develop an interest in cyber security before joining the programme. Furthermore, interviewing participants belonging to the CG allowed us to gain deeper insights into how the lack of participation in the CCIT affected their cyber security interest. It was also essential to see how other factors influenced cyber security interest in the absence of the programme. Finally, interviewing participants belonging to the TG was undertaken to receive a full and direct explanation of how the CCIT was enacted and how it shaped their interest in cyber security and related career aspirations.

[19] See for example Weinhardt et al. (2017) for a study on outcomes of a large-scale multilevel economic and food security Intervention on HIV vulnerability in rural Malawi.

4.3.2.2.2 INTERVIEW SCRIPT PREPARATION AND PILOT PHASE

According to Kvale (2007b), there are no general prescribed rules for interviewing but broad guidelines that can be followed. In line with Kvale (2007b), I prepared an interview script along two dimensions: thematic to ensure valuable data for the research scope were gathered and dynamic to ensure the interaction with interviewees could run smoothly.

Before the first data collection, an interview script was drafted and tested in a small pilot study. The pilot, which occurred between January and February 2020, involved the same participants who tested the survey instrument. More than for the survey questionnaire, the pilot highlighted several challenges which had to be addressed with a wholly revamped interview script. It underlined that more emphasis was needed on questions about participants' motivations and sentiments regarding computer science and cyber security rather than factual queries, even though some were essential to establish a baseline. Therefore, background questions were reformulated to collect more relevant data on students' feelings, motivations, and experiences while ensuring that background information was also gathered.

The initial questionnaire assumed a prior and explicit interest in cyber security, but pilot interviews showed several nuances partially challenging this assumption. While all participants showed a certain degree of interest in cyber security, this varied considerably. Students' attendance in the CCIT had led to assume that they should have had a high level of cyber security interest and knowledge. In reality, participants did not display that because of the admission process criteria. To be selected, students did not need any prior cyber security knowledge. The admission was based on a series of logic and programming questions requiring no specialized knowledge in reverse engineering, hacking or malware analysis. Hence, it was possible for students with varying levels of experience and interest in cyber security to be admitted (or not) to the CCIT. This meant that questions had to be partially reformulated to consider these varying levels of cyber security

interest and experience while ensuring that the interview script was specific enough to gather relevant information for this research.

Furthermore, some questions were reformulated to better evaluate the CCIT's broader objectives and students' motivations to attend. In particular, it became clear that the main focus of the CCIT (or at least the 2019 edition) had not been on cyber security careers but rather on cyber security knowledge and skills development. This was made explicit by the fact that, out of three months of training, students had received visits from industry professionals only once or twice. Only one of the pilot students, who had been selected to compete in the final national challenge, reported that the CCIT had organized a more "structured" career fair at the end of the national final, where approximately ten firms had been invited to discuss cyber security careers. More generally, pilot interviews also made evident that students' primary motivation to enter the competition was to increase cyber security skills and knowledge rather than their understanding of cyber security careers. Thus, the interview script added more questions on the CCIT learning process while keeping an important part of it dedicated to cyber security career interest given its importance in the context of the cyber security skills shortage.

The second interview script was created following the first data collection phase and included results from the first survey, but above all, the first round of interviews. While the first transcript centred around cyber security interest formation and development, the second transcript focused more on the CCIT, its implementation and how it affected cyber security interest.

Both interview scripts were first redacted in English and later translated into Italian to ensure CCIT participants effectively comprehended them. They can be found in annex IV for further examination.

4.3.2.2.3 RECRUITMENT AND DATA COLLECTION PROCEDURES

Following the overall research design, qualitative data were collected before the CCIT training programme and after the final national competition.

The first "pre/before" interview phase occurred from March 4 to April 2. Interviewees were recruited through the pre-survey launched in February. The survey asked participants who were willing to participate in this research to send an email and state their availability. To incentivize participation, €20 vouchers were offered to all participants willing to complete both surveys and be interviewed twice. Out of 965 who replied to the survey, 370 (38%) participants sent an email. Participants were selected on a first-come, first-served basis and according to a set of criteria. Essential criteria were:

- *Location of admission test*: Participants must have sat the admission test in different universities. This criterion was crucial for selecting participants from the TG as training at different universities could have shaped their CCIT experience differently.
- *Geography*: Participants must have come from all three Italian regional groups: North, Centre and South.[20]
- *Gender*: Participants must have been male (8/10) and female (2/10). Even though females were only 12% of survey respondents, it was decided to have at least two females per group. However, while the recruitment of two females in the CG succeeded, unfortunately, it failed for the TG.[21]

[20] North (Emilia-Romagna, Friuli Venezia-Giulia, Liguria, Lombardia, Piemonte, Trentino-Alto Adige, Valle d'Aosta, Veneto); Centre (Lazio, Marche, Toscana, Umbria); South (Abruzzo, Basilicata, Calabria, Campania, Molise, Puglia, Sardegna, Sicilia). This repartition is based on the "Groups of regions" of the First-level Nomenclature of Territorial Units for Statistics of the European Union. For organization purposes, the two Nordic group of regions ("Nord-ovest" and "Nord-est") were merged into one region ("North"); likewise the Islands Group region (Sicilia and Sardegna) was merged into the "South" region.

[21] Only 7% (24/332) of participants admitted to training who completed the survey were female, and none of them either sent an email stating their availability or booked an interview when asked to do so.

- *Level of education*: Participants must have been a combination of high school and university students.

Other selection criteria that were taken into account to make sure interviews could report on several different experiences were:

- Type of high school and/or university department
- GPA
- Parents' monthly income
- Parents' previous study or work experience in IT-related subjects
- Prior enrolment in a cyber security course
- Methods of cyber security knowledge and skills learning
- Number of cyber security competitions previously attended
- Reasons for signing up

The before interview phase took place from 3 March to 2 April 2020. In this first data collection phase, 21 interviews were conducted, 11 with participants from the CG and 10 with participants from the TG. In total, the first data collection phase produced 780 minutes of recordings and 79,506 transcribed words.

TABLE 8 CG FIRST INTERVIEWS

Control group		
Participant	**Interview length (min)**	**Number of transcribed words**
Avan03	38	4,408
Boel22	41	5,208
Caed14	29	1,998
Caid06	32	2,868
Molo31	42	5,107
Most17	54	7,229
Pede20	39	3,562
Pola07	37	4,246
Ropa25	33	3,947
Stma02	26	-[22]
Trma18	55	7,201
Totals	**426 min**	**45,774**

TABLE 9 TG FIRST INTERVIEWS

Treatment group		
Participant	**Interview length (min)**	**Number of transcribed words**
Anri23	26	1,859
Cani30	52	6,599
Fopa06	32	2,395
Gama26	31	2,414
Gari24	36	3,142
Maan10	34	3,744
Mami07	28	2,553
Mona29	30	2,976
Rose07	45	4,718
Udel09	40	3,332
Totals	**354 min**	**33,732**

The “post/after” interview phase took place from 6 to 27 October 2020. From 6 to 15 October I interviewed the participants who had been interviewed in the first data collection phase. Unfortunately, three participants from the TG dropped out of the research, providing no explanation. Moreover, one participant moved from the TG to the CG as he did not undertake the training. Therefore, 18 interviews were conducted, 12 with participants belonging to the CG and 6 with TG participants.

An added design element of this research was the recruitment of additional interviewees through the second survey. One survey question directly asked respondents, “Did the CCIT influence your interest in cyber security?” If

[22] This interview was not transcribed as data quality was strongly below the standards of previous interviews and would have not generated any novel insight, which all other interviews did.

respondents answered either “The CCIT has significantly decreased my interest for cyber security” or “The CCIT has significantly increased my interest in cyber security,” they were redirected to a survey page asking to send an email and state their availability to be interviewed. This design element was added to ensure this research could report on experiences that the CCIT profoundly shaped, hoping that these interviews could highlight even more what factors contributed the most. To incentivize participation, €15 vouchers were offered to participants who had completed both surveys and were willing to be interviewed.

For the second data collection phase, 29 interviews were conducted, 16 with participants from the CG and 13 with TG participants. These interviews produced 961 minutes of recordings and 101.753 transcribed words.

TABLE 10 CG SECOND INTERVIEWS

Control group		
Participant	**Interview length (min)**	**Number of transcribed words**
Avan03	28	2,773
Boel22	24	2,514
Caed14	20	1,585
Caid06	17	1,493
Cuem16	25	3,032
Mami07	16	1,348
Molo31	20	1,989
Most17	41	5,588
Pahe07	28	3,520
Pede20	22	2,033
Pido06	49	4,903
Pola07	31	3,368
Ropa25	20	2,219
Rost20	26	2847
Stma02	13	717
Trma18	34	4,022
Totals	**414**	**43.951**

TABLE 11 TG SECOND INTERVIEWS

Treatment group		
Participant	**Interview length (min)**	**Number of transcribed words**
Anri23	16	1,522
Cani30	41	5,234
Cesi28	47	4,715
Czro19	31	3,486
Gama26	30	2,319
Gari24	27	2,719
Moma11	117	12,166
Mona29	29	3,234
Pano15	57	6,418
Pgro17	45	5,302
Udel09	24	2,152
Vegi07	48	4,784
Vida12	35	3,751
Totals	**547**	**57.802**

To summarize (table 12), I conducted a total of 50 interviews with CG and TG participants:

- 21 interviews were conducted in the first data collection phase, and 29 in the second phase;
- 27 interviews were undertaken with participants from the TG, and 23 with participants from the TG;

- The first and the second data collection yielded approximately 29 hours of recordings and 181 thousand words transcribed;
- A total of €525 (£473) worth of vouchers were awarded to incentivize participation.

TABLE 12 SUMMARY OF INTERVIEWS

Summary of interviews:
1st data collection:
▪ **11 students in CG** ▪ **10 students in TG** ○ **Total interviews in 1st data collection: 10+11= 21**
2nd data collection:
○ **Students who took part in 1st data collection and 2nd data collection:** ▪ **12 (CG)** ▪ **6 (TG)** ▪ **Total: 18** ○ **Students who took part in 2nd data collection only:** ▪ **4 (CG)** ▪ **7 (TG)** ▪ **Total: 11** ○ **Total interviews in 2nd data collection: 18+11= 29**
Total interviews (1st and 2nd data collection):
▪ **CT: 11+12+4= 27** ▪ **TG: 10+6+7= 23** ▪ **CT+TG (27+23) = 50**

Data collection and management was assisted using three different software:

- Interviews were conducted and recorded via Skype, which is considered an effective tool for qualitative research (Deakin & Wakefield, 2014; Lo Iacono, Symonds, & Brown, 2016). Skype was chosen over other services mainly because it is free, generally well-known, and easy to record calls with;
- Data were transcribed with Trint, an automated transcription software, to speed up the process and leave more time to the analysis; [23]
- Data were managed and analysed in NVivo because of features, such as auto-coding function, which enabled the process to be generally more organized and rigorous.

4.3.2.2.4 QUALITATIVE DATA ANALYSIS

Qualitative data analysis blended methods and insights by Braun and Clarke (2006), Gibbs (2007), Jackson and Bazeley (2019) and Spencer, Ritchie, O'Connor, Garreth and Ormston (2014).[24] These authors do not subscribe to any particular theoretical or methodological doctrine, although they do not seem far apart from the main elements of grounded theory (Flick, 2018). The benefit of resorting to their methods is that they pin down qualitative data analysis on a practical level, which is particularly suitable for the qualitative component of this thesis, whose aim is not to create a theory but rather to understand processes and behaviours associated with cyber security interest formation and skills competitions.

Regarding the data analysis process, I followed Braun and Clarke's steps of thematic analysis, which minimally organizes and describes data sets in detail.[25] The process comprised of five steps:

[23] https://trint.com/
[24] These approaches were chosen following careful consideration of other methods as outlined by Flick (2018), Kvale (2007a) and Silverman (2015).
[25] Braun and Clark's core elements are in line with those of Gibbs, as they define thematic analysis as "a method for identifying, analysing and reporting patterns (themes) within data," and their data

1. I familiarized myself with the data, which involved producing the transcripts, transferring them into NVivo and organizing them. I then read them several times and annotated how my analytical understanding of the data evolved through memos;
2. I created an initial "thematic index," which had been made easier by the semi-structured interview scripts used in the data collection process. This allowed later the auto-code function in NVivo, which helped generate an initial index based on the questions of the interview script;
3. I started generating the initial codes and sorting them into the above themes so that all relevant data were placed into one "thematic box;"
4. I reviewed the ensuing themes. After making sure all codes were coherently allocated within each box, they were revised and refined.
5. I defined and renamed the themes, seeking to understand how they linked together in answering the research questions.

The generation of codes was probably the most relevant phase during the process, and therefore it deserves to be further unpacked. Coding defines "what the data you are analysing is about. It involves identifying and recording one or more passages of text or other data items such as the parts of pictures that, in some sense, exemplify the same theoretical or descriptive idea" (Gibbs, 2007, p. 38). During this process, I sought to link the passages found in the interview transcripts and unite them under a common theme. Coding was a way of categorizing the text so that the large amount of data collected could be read (or interpreted) through a thematic framework of ideas, thus allowing to "recontextualize" the data (Telsch, 1990). It was not a mechanical task as it required continuous revaluation and rethinking, making it an integral part of the analysis process (Jackson & Bazeley, 2019). This implied "intensive reading" with some basic questions that helped me think throughout the task (Charmaz, 2003, pp. 94–95):

analysis procedures are comparable to those of Spencer, Ritchie, O'Connor, Garreth and Ormston (2014).

- What is going on in this passage?
- What is the participant doing and saying?
- What do these actions and statements take for granted?
- How do structure and context support, maintain, impede or change these actions and statements?

In terms of what to look for, Gibbs states that there is some consensus on what researchers tend to look for when doing qualitative analysis, especially in policy and applied research. Moreover, Jackson and Bazeley provide valuable insights into strategies to identify and label codes. The table below (n. 13) shows what elements I initially looked at when I approached the data for the first time and started to develop my analytical journey:

TABLE 13 CODING STRATEGIES

Gibbs (2007)	Jackson and Bazeley (2019)
1. **Specific acts and behaviours** 2. **Events** 3. **Activities** 4. **Strategies and practices** 5. **States** 6. **Meanings** 7. **Participation** 8. **Relationships or interactions** 9. **Conditions or constraints** 10. **Consequences** 11. **Settings** 12. **Reflexive**[26]	1. Look for repetitions and regularities 2. Use questions of the text to generate codes 3. Compare and contrast passages of text 4. Compare data with hypothetical or extreme examples 5. A priori, or theoretically derived, codes 6. In vivo, or indigenous codes

[26] The list is adapted from (Bogdan, R.Biklen, & S.K, 1992; Mason, 1996; Strauss, 1987)

While generating codes and refining themes, the process from “seeing” to “seeing as” was the most important. “Seeing” occurred when I noticed patterns in the data; classification and description followed. Instead, “seeing as” consisted of noticing and finding links among the identified patterns (Boyatzis, 1998, p. 4). Finally, I ended the coding process when the material stopped generating themes or ideas anew.

One of the criticisms levelled against qualitative research when presenting the findings is that publications seem to be often anecdotal, “giving the reader little guidance as to the prevalence of the issue to which the anecdote refers” (Bryman, 2015. In this context, brief sequences of conversation or snippets of transcripts provide little sense of the prevalence of a certain theme, with the risk that particularly impactful statements or examples are highlighted more than might be warranted in terms of its frequency. To avoid that, whenever a theme emerging from qualitative data is presented, I provided a rough indication of the number of interviewees mentioning it.

4.5 Ethics

As this research involved human participation and the collection of personal data, there were ethical issues that had to be tackled to ensure this study followed appropriate research standards. This section describes these ethical considerations, which were submitted as a CUREC application form to (and approved by) the Department of Education’s Research Ethics Committee.[27] In designing the approach to ethical research, this study adhered to the British Educational Research Association Ethical Guidelines for Educational Research and followed Oxford University’s best practice guidance, in particular BPG04 (Competent youths), BPG06 (Internet-based research) and BPG09 (Data

[27] A copy of this form can be found in annex V.

collection, protection and management). The primary ethical concerns were related to recruiting underage study participants, obtaining consent, and storing personal data.

The main potential issue that this research had to consider was collecting data from "children" aged between 16-17 years old as the CCIT recruited individuals aged 16-23 years old. However, following Oxford University's best practice guidance "BPG 4 Competent Youth,"[28] it was determined that the purpose of this study qualified them as "competent youth." The university's guidance suggests that studies on attitudes towards science and mathematics could involve "competent youth," namely individuals who are aged 16 and 17, who hold the legal status of children in the UK and the EU, but who have sufficient understanding of the project's content and its implications for them. In the science education field, interest is a topic that is usually incorporated in the broader literature on attitudes towards STEM disciplines and careers. As the leading research goal was about determining cyber security interest and how the CCIT influenced it, it could be assimilated to a study on STEM attitudes, and therefore CCIT participants were considered "competent youth."

The second main concern was obtaining participants' consent. As this research collected data through multiple methods, consent had to be gathered in different ways. Prior to accessing the surveys, study participants were asked to read a research and privacy note, which included all the relevant information regarding:

- Who was leading the research
- The research rationale
- Why individuals were asked to participate

[28] https://researchsupport.admin.ox.ac.uk/files/bpg04competentyouthspdf-0. Further information was also gathered from Approved Procedures A15 ("Teachers and teaching in educational setting") and A25 ("Non-invasive research methods with children).

- Whether or not they had to take part
- What happened if they took part
- The potential risks and benefits
- What would happen to the research data
- Whether the research would be published
- Who approved the research
- Who to contact for lodging a complaint
- Data protection information

At the end of this note, participants had to tick three boxes declaring they 1) were 16 years old or above; 2) understood the study purpose and how data were stored and analysed; 3) knew whom to contact to get more information or lodge a complaint. The research information and privacy note can be found in annex VI.

This research also collected data from interviews, which needed a different form as specific consent to record them through Skype had to be asked. After the recruitment process, I sent a research information note and a consent form to the study participants, which they had to sign before the day of the online meeting. Moreover, if study participants were below 18 years old, their parents had to sign the consent form as well. The interview consent form can be found in annex VI.

Even though this research did not collect or discuss sensitive data, the third main critical element was storing research and personal data:

- *Survey data*: survey responses were collected through Jisc Online Surveys, which was chosen because it complied with the EU General Data Protection Regulation. Study participants were asked to create a unique identifier in order to verify how many replied to both pre and post surveys. However, it is impossible to trace the unique identifier/research data to the respondent as the survey did not ask to insert any additional personal information linked to the respondent's identity. Survey data were downloaded and stored on an encrypted USB drive.

- *Interview data*: interviews were recorded through Skype, which automatically deleted all recordings after 30 days. Interviews were transcribed using Trint. Once interviews were transcribed and edited, they were permanently deleted. The interview transcripts were then stored on an encrypted USB.
- *Contact details*: participants who were interested in being further involved in the research through interviews voluntarily sent an email to a Gmail account expressly set up for this research. Participants' email addresses were stored on the mentioned email account, which was password-protected, and not transferred anywhere else. The only personal data (i.e. email addresses and participants' name/surname) transferred were those of individuals who were then selected to participate in the interviews. Their data were stored in a password-protected Excel file on an encrypted USB drive.
- *Interview consent forms*: To be interviewed, participants had to sign and send a consent form, which was stored on an encrypted USB drive.

Research and personal data were accessed by the researcher only, and they were not shared with any other organisation. They will be deleted three years after the thesis is deposited in the ORA University archive per Oxford University's regulations.

4.6 Summary of methodology

This research aimed to analyse cyber security interest development through the lenses of national cyber security competitions. To limit the scope of the inquiry, it considered only those NCSSCs whose national teams attend the ECSC. It selected the Italian CCIT as a case study because it is the NCSSC in Europe that trains the largest number of participants for at least three months, and therefore its influence on participants' interest is likely to be more observable.

In light of the CCIT's structure, this research was designed as a before and after study. Data were gathered before the start and at the end of the competition from a control and a treatment group. This research employed mixed-methods of data collection and analysis to achieve its objectives. Overall, the mixed-methods design was convergent, whereby quantitative and qualitative data were combined to interpret the results holistically and answer the third main research question of this thesis ("Is an NCSSC an effective policy to address the shortfall of cyber security professionals in the labour market?).

The quantitative element of this thesis had the primary goal of discovering the extent to which the CCIT exerted an influence over participants' cyber security interest. As several studies had already attempted to examine interest, this thesis relied on existing survey instrument items, even though they were amended to suit the specificity of this research. The pre-to-post research design implied that surveys were sent before the start of the CCIT and at the end. While the first survey had a reasonable response rate, the second one did not receive enough responses from the main comparisons groups. Because of the insufficient sample size, lack of randomization in the allocation process, and highly skewed data, it was decided to employ data mainly for descriptive purposes and to highlight emerging themes and trends. In light of these issues, the qualitative element of this research assumed an even more significant role.

The qualitative component of this thesis had the objective of explaining how CCIT participants developed an interest in cyber security before taking part in the skills programme and how the CCIT influenced their interest. Qualitative data were collected through one-on-one Skype interviews with control and treatment groups participants. To follow the before and after design, interviews were conducted before the beginning of the CCIT and at the end. It is the first time this method was employed in a study on skills competition and interest development. Study participants were recruited through the first and second surveys and according to a set of criteria to ensure that the widest variety of CCIT experiences were accounted for. In total, this research conducted 50 interviews, which generated

approximately 29 hours of recordings and 181,000 transcribed words. Data were transcribed with an automated transcription software, and later organized and analysed with NVivo. Qualitative data analysis took inspiration from the work of several authors but followed more closely Braun and Clarke's process.

Critical ethical issues such as recruiting underage study participants, obtaining consent, and storing personal data were addressed with a CUREC application form before the data collection process.

If one includes expenses for the pilot phase, participation incentives in the form of Amazon vouchers, and the transcription software, this research had a total budget of £2.302.

5. The development of cyber security interest

This thesis has four findings chapters:

- *Chapter 5* gathers data on how CCIT participants became interested in cyber security. Doing so highlights the "triggers" that contributed the most to the development of this interest. To better understand the context in which cyber security interest was formed, this chapter also identifies the factors that made students passionate about technology and computer science. This chapter answers the first main research question: *How do participants develop an interest in cyber security before attending a NCSSC? What factors specific to cyber security may trigger the development of such interest?*

- *Chapter 6* aims to establish CCIT participants' cyber security interest before the beginning of the CCIT. This is an essential step to understanding the extent to which their interest changed during the programme, which is the goal of chapter 7.

- *Chapter 7* finds out the extent to which participants' cyber security interest evolved during the programme. This chapter goes beyond the concept of interest by presenting results on other essential variables such as education and career planning, key choices in education paths and careers, and the relation with competing interests. This chapter is central to the whole thesis as it provides the required evidence for a complete discussion on the benefits and disadvantages of a national cyber security skills competition as a shortage mitigation policy. Together with chapter 6, it answers the first part of the second main research question: *Do NCSSCs influence participants' interest in cyber security as a topic and as a career?*

- *Chapter 8* explains how participants' interest changed during the CCIT, describing how the programme was enacted and highlighting the major elements that influenced students' interest, in particular the admission process and the training programme. This chapter helps identify the factors that, according to participants, are more likely to make a national cyber security skills competition "successful" in increasing interest. It answers the other part of the second main research question: *How do NCSSCs influence participants' interest? What factors contribute the most to influence interest?*

Chapter 5 aims to identify the main factors contributing to the development of cyber security interest among participants before the beginning of the CCIT. This chapter answers the first main research question "*How do participants develop an interest in cyber security before attending a NCSSC? What factors specific to cyber security may trigger the development of such interest?"* by using data collected from the first round of interviews and the two surveys. To better understand the context of cyber security interest formation, it also digs deeper into the origins of students' passion for IT and computer science. The findings are helpful to put in perspective the next chapter, whose goal is to establish a baseline of CCIT participants' cyber security interest before joining the Italian cyber skills competition.

This chapter is divided into three main sections:

- Section 5.1 investigates the process through which students started to use technology and became passionate about computer science topics and skills;
- Section 5.2 presents the main factors that contributed to developing interest in cyber security;
- Section 5.3 summarizes the findings of this chapter.

5.1 Interest in technology and computer science

The first section of this chapter explores the origins of CCIT participants' technological and computer science interests. This section helps to contextualize the results of section 5.2 as for most CCIT participants interest in cyber security did not just happen in an instant. Instead, it was the culmination of a lengthy process of interest development in technology and computer science that had started from an early age. This also explains why CCIT participants might not consider cyber security their sole and primary interest, as shown in section 7.5.

5.1.1 Videogames, school activities and access to technology

Almost every interviewee started using computers relatively early, usually between four and ten years old. This happened for two main reasons: to play video games and for learning purposes. Moreover, an "environmental" element helped them to develop their attraction for IT tools, namely easy access to technology.

Most study participants initiated their journey into the discovery of computing through videogames and other ludic entertainments such as Microsoft Paint. Starting from these games or other similar recreational activities, they developed a curiosity about the medium that allowed them to have fun, which progressively led them to become more interested in how the computer and its main components worked.

For example, one student remembered that:

> "(…) since I was little, I was attracted by these technological objects which were like gold to me (…). If I am not mistaken, dad allowed me to play with a videogame on a very old laptop, it was 2006 or 2007, I was three or four years-old (…). [After playing] I told myself, I must understand how it works, this is too fun…"

Similarly, another student explained that he had started using a computer because he enjoyed playing at a videogame called Minecraft. He then developed an interest

in the inner workings of a computer, which spurred him to continue studying computer science.

Nevertheless, video games were not the only reason students started using laptops. Some students started using them to accomplish school tasks, with many of them having their first experiences in primary school, where they were taught the basics of Microsoft Office. For instance, one participant was introduced to computers in his first elementary school years, when coursework required him to perform internet searches. Later, he learnt how to use Word, Excel and PowerPoint.

While videogames and school tasks were the main reasons students started using computers, there is also an environmental reason that facilitated this interest to develop, namely easy access to parents' IT equipment. This did not mean that parents were necessarily working in the IT sector, but rather that they were using computers for professional purposes and allowed their children to approach technology in a controlled environment.

For example, a participant's father was an engineer who had always used computers to perform his job. When the student was around five years old, she started accessing her dad's computer to use Microsoft Paint. Therefore, she had already started to use this technology even before commencing elementary school.

Another student had always been using a computer because he had been surrounded by them since he was little, noting how his parents were using them to run their business.

5.1.2 From videogames to computer science

Videogames and educational activities allowed interviewees to have their first early experiences with technology, but this does not entirely explain how their interest and expertise in computer science grew over the years. In fact, these two activities can probably describe how many young individuals started using technology. One factor explaining how they developed a more substantial interest in computer science was CCIT participants' innate desire to understand how computers worked from both a theoretical and practical perspective.

One student became attracted to computers because they could do things that he "could not even imagine," and he wanted to understand how they functioned. After realizing that his computer was often slow, he tried fixing it and understanding why it was not operating properly:

> "At this point, I switched from playing with the computer and waiting for it to work, to understanding why it was not working. I got interested in how it worked inside."

Another student narrated his childhood experience and how his uncle's ability to fix computers captivated him. When his parents had computer issues, he remembered that his uncle would come to the rescue and initiate a remote connection. He liked seeing the mouse cursor moving and the home screen changing despite no one touching the computer on his end. As he could not understand how his uncle could do it, he felt a strong desire to know more about how computers were made and functioned.

A student stated that his passion for computer science had come out naturally, and from then on, he kept cultivating it. He approached it slowly and started to ask himself the rationale of laptops "like a child who asks why all the time."

This attraction for IT technology usually grew steadily and was characterized by routine computer usage that cemented students' interest over the years. CCIT participants employed computers for entertainment and school purposes.

However, what probably distinguished them from other young users was their early approach to programming and IT experiments. One can argue that it was a mix of gaming, school usage, programming and self-experimentation that consolidated their interest and increased their expertise in computer science matters.

One student described himself as “being born with a computer in his hands” and to have always liked exploring what was possible to achieve with it. He started programming when he was in middle school and, after video gaming with friends, he used to think of what software to create. He usually drew inspiration from YouTube or school lectures. For example, one day after a physics class, he and his friends did a project in JavaScript to reproduce what they had learned in class about the harmonic motion.

Another student explained that he sought to improve his knowledge once he became interested in IT. So, he started to download and install software, change the operating system or enter the system BIOS to observe how the system would react. Some of his experimentations did not go as expected (“I did some stupid stuff such as changing the operating system and replacing it with Android...I created two partitions, but by mistake I overwrote the Windows partition, and so I let you imagine what happened”) but all this had helped him to achieve a more nuanced understanding of systems and networks.

The example of how a student coupled his growing passion for computer science with a very practical need (due to his condition as a visually impaired individual) was interesting in showing the complex interplay contributing to the development of interest. He revealed that he had been learning advanced computing since he was little (“I mean, when I was in middle school I was easily managing a Debian server already”), as he had understood from the beginning that a PC could help him greatly in his life and work. From that realization, he described how he went from Microsoft Word to manage complex IT systems:

> “At the beginning, the [computer] usage was mainly due to school, therefore writing and reading documents, namely using Word. After that, slowly, from Word, I started to have a stable internet connection (…), so YouTube and

> some emails (…). I started programming when I was in my second year of middle school. I started to deal with systems before (…) and then with the first bash commands (…)."

Finally, one interviewee explained that his passion for gaming made him study computer science in-depth because he wanted to understand how the various PC components worked. This aspiration to know more about the inner workings of a computer led him to assemble one on his own when he was very young. Then, this interest moved to the software side, and he started programming.

5.1.3 Family members and their influence

A potential factor that could explain interest development in some students, especially at an early age, is the direct or indirect influence that close family members exert (Dunst & Raab, 2006). While some study participants described how interest in technology had been "handed down" to them by their parents, most interviewees developed a genuine passion for computer science on their own. Regardless of this direct or indirect influence, participants were undoubtedly supported by their families in their choice to pursue computer science.

Approximately two-thirds of the interviewees declared that family members had not directly influenced them as they did not have either the educational background or the affinity with technology to do so.

One student reflected that her parents' economic and educational background did not have a bearing on her computer science education. She explained that her parents did not come from well-off families and never really went far in their academic studies ("They are workers, they do not have this [computer science] knowledge, they never studied it") and therefore, her passion for computers had come directly from her.

Another student referred to the fact that his parents did not fully understand what he was doing, and therefore they would have been unable, had they chosen to try, to convince him to abandon computer science. He had always been the one

making the decisions about his education, and his parents have always supported him. While they might have had a role in helping him choose the right high school, from then on, they did not have any impact on his decision-making: “my parents do not have the understanding of what I am doing because obviously a person who has middle-school level math (…) is not really able to (help me) take these decisions.”

One student defined his parents as “very distant” from technology because they did not understand it, even though they might use it for work. I asked him if he could explain why his parents were so apart from technology and how he, on the other hand, became so attracted. A possible explanation was that he had never seen technology until a certain age and, once he realized its potential, he started to appreciate it more and more.

One example was particularly striking in highlighting that, even when conditions were clearly favourable for students’ interest to be shaped by a family member, this did not occur. A participant’s uncle was the founder of a cyber security company, and one would think this could have greatly influenced the student to pursue computer science first and then cyber security. However, the answer the student gave was unexpected: “[My uncle] did not influence at all my interest because my interest was born before I knew about his professional activity.” He admitted that his uncle had advised him to persevere in his studies, especially cyber security. Nonetheless, he declared that there had been no occasions to exchange ideas or work together since then.

The finding that overall CCIT students had not necessarily derived their IT interest from their family members is also backed up by survey data (N=895), whose results showed that only 18% of participants’ parents had studied IT subjects[29] and only 15% had had a job in the IT sector (figure 11).

[29] Defined in the survey as computer science, computer science engineering, electronics, telecommunications and cyber security.

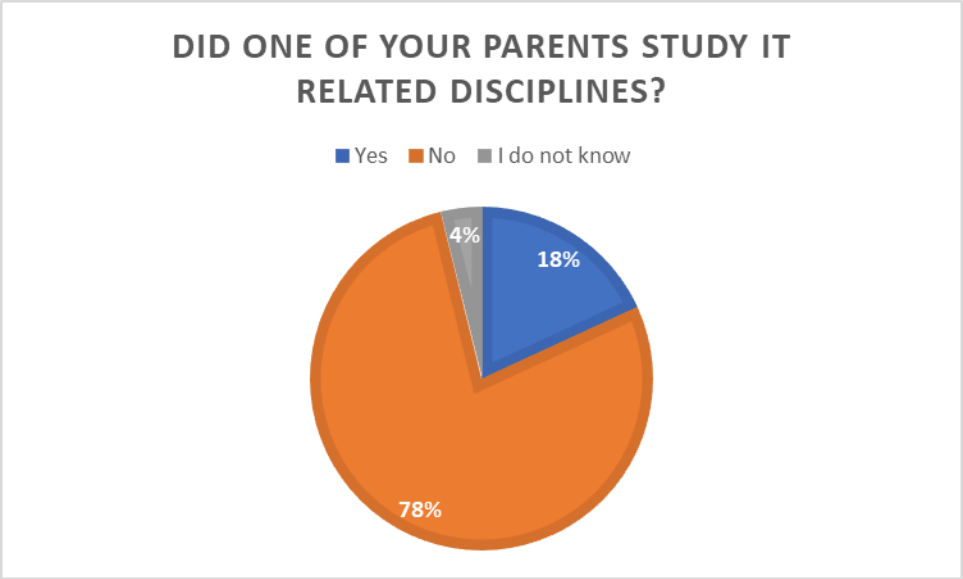

FIGURE 11

On the other hand, however, approximately one-third of interviewees had their interest in computer science directly influenced by family members. Usually, the father had the most substantial impact, and this shaping dynamic occurred when students' interest was forming between elementary and middle school.

The most straightforward example was one where a father used to work in the IT unit of the armed forces, and the brother was a programmer. The student gave a candid explanation of how he started using computers: "I do not know precisely, they told me "Do you wanna try doing computer science?" I said yes, I started doing computer science, I liked it, and I carried on."

For another student, it all began when he started sitting next to his dad while he was using his laptop. The two would sit together and do educational activities on the web. It was through his father that he developed a strong familiarity with technology. His interest was then cemented by visiting his cousin over the summer, a computer science-engineering student. When the cousin was working on his

computer, the interviewee used to go and sit next to him. He clearly remembered being thrilled by many of the things his cousin was doing.

The explanation of how a student took his father hobby and turned it into his passion was fascinating. When he was around eight years old, he started observing his dad, who had always been passionate about computers, and he got closer to the computer world: “I transformed his rudimentary way of dealing with technology into my passion, but much more rooted and deeper.” He had an interesting account of how his father’s relationship with technology influenced his: “[My interest for computer science] got worse because he taught me to look at computer science with interest but also with a bit of fear because while computer science shows a nice world of progress, there is also the other side of the coin, which is what happens when computers are wrongly used. So, it’s about it, it became a sort of a question of respect for this very very particular world.”

Another participant explained that her father was crucial in building her confidence. She mentioned that her dad used a laptop for his engineering work, and when he was young, he had some early exposure to coding. Thus, it was vital for her to go to him and ask for support when she needed it:

> “… he did not dismiss me or told me to do it myself. He would stay close to me and try to help, to understand, even though he might have been struggling as well because he had not studied programming further, but he would try to help me. I think it helped me a bit the fact that he had always been supportive…”.

Regardless of this family influence, an interesting and solid finding was that CCIT participants have always been supported by their family members in their choice to pursue computer science. This is an important factor as it is not difficult to see that, if family members had been opposed to their choices, this could have fatally hindered the development of participants’ computer science interest.

In the first survey (N=895), 69% of students thought that their family had encouraged them to study computer science.

Interview data found that interviewees' parents and other family members have been even more supportive than the survey data suggested. Although economic considerations have always been important, parents strongly supported their children in their quest.

For example, one student reflected that the only consideration that her parents ever made was economic. Their only concern had always been her having to move to more expensive cities like Milan or Rome, but apart from that, "they only want me to conclude [what I started]." She described her parents as "very practical," and hence, as long as she was able to show them she could get to the end of her studies and financially sustain herself afterwards, they were happy with the choice.

Another female colleague made a similar point about the freedom she was granted to choose her path. She claimed that there had never been any issue in choosing computer science, if that was the path she wanted to take. When she started to express her interest in a master's degree in cyber security, her parents were aware it might have been difficult for her to get admitted or that she might have had to move to a more expensive city. Nevertheless, they were still willing to support her: "they would continue to support me, actually they would brag with their friends that I entered (a master's degree) in cyber security. So yes, I think they would fully support me."

5.1.4 Formal education and schooling

Another critical factor that could shed light on the development of interest is the formal education students opted for and received. In fact, it is not hard to hypothesize how a school pupil could be intrigued by a school subject area, which he/she then takes it forward to study at university and potentially makes a career out of it. However, the results below show that most students chose specialized IT schools and degrees to uphold their passion for STEM subjects and computer science and not the other way around. Another interesting finding is that

approximately 40% of interviewees had been unsatisfied with the education they received, which led them to autonomous learning.

The first survey (N=895) found CCIT participants to be almost evenly split among high school (47%) and university (52%) students (figure 12).

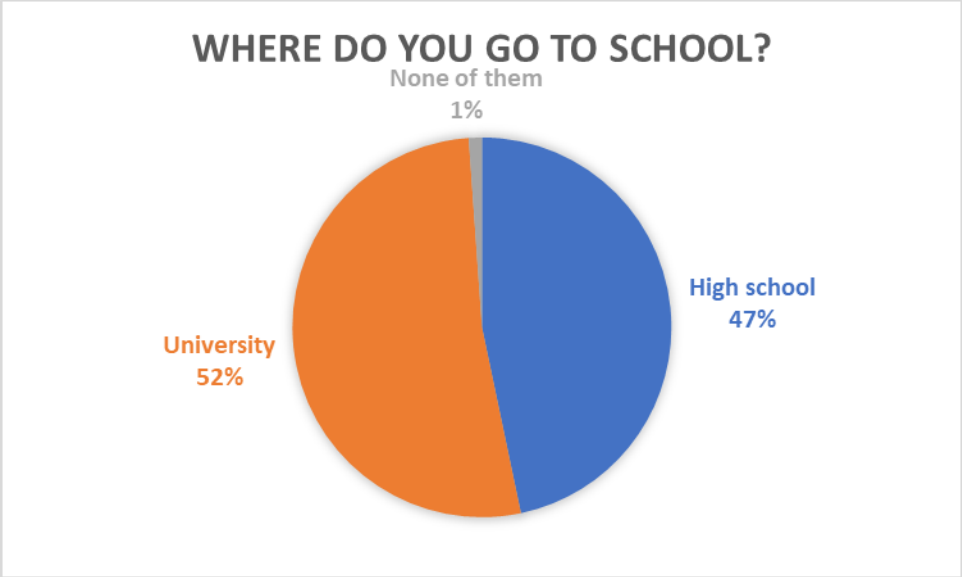

FIGURE 12

High schoolers were most of the time enrolled in technical institutes (64%), followed by lyceums (34%) and professional institutes (2%) (figure 13).[30]

[30] The Italian secondary education system comprises three types of high schools:

- Liceo (lyceum), which typically prepares students for university;
- Istituto tecnico (technical institutes), which still qualifies students to enter university, but generally covers more technical and practical subjects that are linked to sectors that are "fundamental" for Italian economic development;
- Istituto professionale (professional institutes), which entails practical work related to a specific industry or trade (Ministero dell'Istruzione, 2021b)

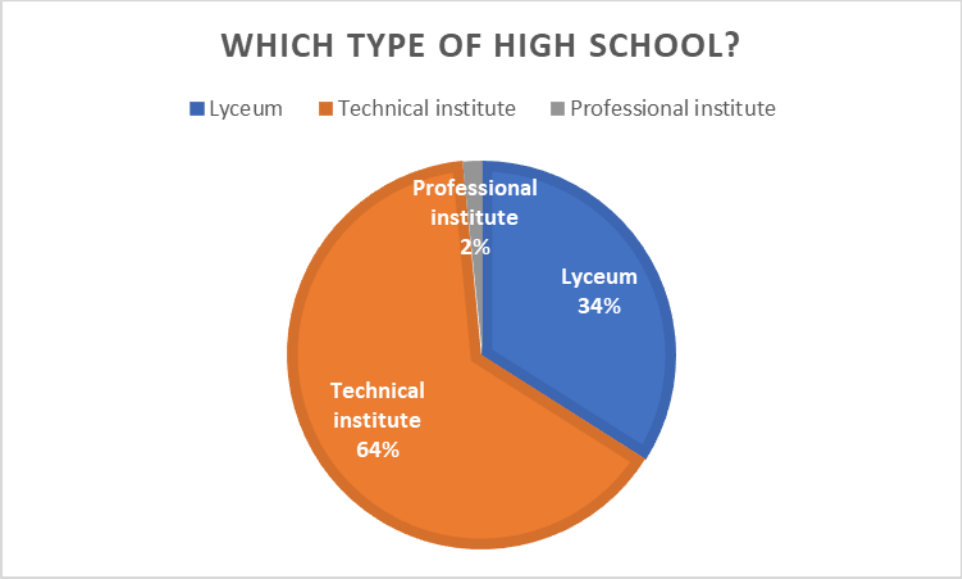

FIGURE 13

Participants who attended technical institutes were overwhelmingly enrolled in the "computer science and telecommunications" curriculum (91%); participants who attended lyceums were largely (73%) enrolled in the "scientific – applied sciences" curriculum, which includes computer science coursework, as opposed to the "traditional" scientific lyceum, which stresses Latin instead of computer science. This means that 84% of secondary education students were enrolled in educational paths which entailed compulsory computer science education.

Secondary education students who replied to the first survey claimed to have an excellent GPA: only 15% had a GPA lower than 7.00; 37% had a GPA between 7.00-7.99; finally, 48% said to have a GPA above 8.00, which is a high GPA in Italy.

Among university students, 81% were enrolled in a bachelor's degree, and 19% were enrolled in a master's degree (figure 14).

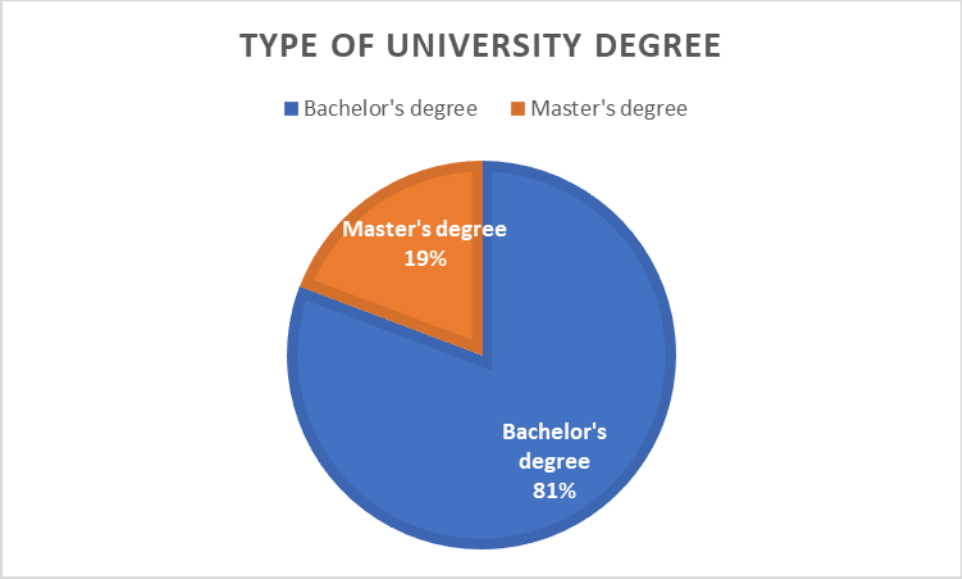

FIGURE 14

Most university participants were enrolled in a computer science degree (76%), followed by engineering (9%), mathematics (6%) and electronics and telecommunications (4%).

University students were also good or excellent students: 39% of them had a GPA above 27 (out of 30), which is considered a very high GPA for STEM degrees in Italy; 39% had a GPA between 23-26 and 22% had a GPGA between 18-22.

5.1.4.1 The rationale behind the choice of academic routes

Interviews were useful to dig deeper into the rationale behind these educational choices. In particular, they helped understand whether interest in computers and IT more generally influenced students' educational choices or whether their school choice enhanced their interest in computer science.

The main reason that drove students to enrol in IT schools and university degrees was their passion for STEM subjects, particularly computer science. This sentiment was widespread among study participants, and one could argue that if

layers of factors formed educational choices, passion and interest towards science topics and computers were the foundational layers on top of which these decisions were built.

For example, one student remembered that he had chosen the scientific lyceum because he had always been attracted to scientific topics in middle school and therefore had decided to continue down this path. He then decided to enrol in a computer science-engineering degree because, while in high school, he had approached the computer science world, and he had felt it was the best choice.

One student declared that his main reason for enrolling in a technical institute was a general passion for everything related to computer science. After high school, he decided to enrol in a computer science-engineering course, which was motivated by the fact that he wanted to have a professional career in this domain and the best way to do this was to get that degree.

Another participant enrolled in an applied sciences scientific lyceum because she preferred scientific subjects such as natural sciences and mathematics. After high school, she enrolled in a bioinformatics course because she loved computer science and programming.

Finally, one student declared she had been happy about her decision to enrol in a scientific lyceum because it confirmed that she liked computer science more than any other subject. She also described the process through which she chose a computer science bachelor's degree: "At the end of my high school, it was August and I did not know what to do. Then, I started to summarize what I did during high school on paper, and I understood that what I liked the most, the thing that I put more effort into and I got the best marks in, was effectively computer science. Then I said, well, now I go to enrol, and I enrolled in a computer science course."

These and many other examples imply that students opted for the school curriculum or university degree that could nurture their passion for computers, IT and STEM subjects more broadly and not the other way around. There was only

one case of a student who seemed to have experienced the opposite, namely his passion for computer science grew after switching from construction engineering to computer science-engineering while at university.

He narrated that he was unsure about which direction to take after high school, so he enrolled in construction engineering. However, after three months, he realized it was not the right degree for him and switched to computer science-engineering: “And so, it is in that moment that I have discovered the passion for computer science, which is something that I had always nurtured, although indirectly. It did not occur to me that much [that I was so passionate about computer science]. Instead, by taking this decision, this passion came out...”. This interest was brought up when in class they started to analyse computers more deeply and from a mathematical perspective: “You become aware of certain processes within a computer that you take for granted which in reality are not. From then, it becomes interesting to analyse how a computer performs certain tasks.”

5.1.4.2 Dissatisfaction with formal education and self-learning

One interesting finding that was brought up by approximately 40% of interviewees was the dissatisfaction with the knowledge and skills that the Italian education system provided, which led them to understand the importance of self-development and autonomous learning.

One student claimed that his high school’s objective was to guarantee that all students could reach a good level of computer science education rather than supporting very interested students. He suggested that the threshold was always put lower, so if there was a program to implement, the task's difficulty was decreased to allow every student to reach the intended level. The student then decided to enrol in a computer science-engineering course because “I was not satisfied with my high school, I told myself, there are more things I can learn.” Nevertheless, even once enrolled in higher education, he realised its limitations, for example, when he noticed a discrepancy between the skills needed to perform

in cyber security skills competitions and those taught in class. He claimed that the people who had profound security knowledge most of the time had to neglect university to acquire that specific knowledge. He made an example of his friend, who was “years ahead” of him in cyber security skills development, but who was also trailing behind in his university career. He concluded that universities would need to increase security coursework to allow students to better understand the subject.

This sentiment was shared by a fellow student, who explained how his experience in skills competitions made him and his team realize the shortfall of their education:

> “… competitions went very badly because we literally did not know what to do (…). We realized how unprepared we were to enter this world, mainly because our main source of information, the school, provided us with theoretical and practical knowledge that cannot cope with the requirements of these competitions. (…) Surely, this brought disappointment because I enrolled in this curriculum because I thought it could prepare me for this world, which is something that in the end it did not do.”

Similarly, this is how a student explained the rationale behind his choice of joining cyber security challenges:

> “Mainly because of curiosity, the fact that cyber security is a field that interests me, but I also preferred to get deeper in certain things that unfortunately you do not do in class. It is not a critique to the university, but in Italy there is a tendency to be theoretical when, at least in certain field, one should be more pragmatic. Therefore, I preferred to do certain topics on my own at a more practical level.”

These limitations of the Italian education system pushed at least one-third of the interviewees to do some extra work at home on their own, allowing them to delve deeper into concepts and practices not taught in school.

One student believed that the ability to learn on your own is essential to excel in this field. I asked him whether schooling or his personal activities made him understand computing more. He ascertained that “it is more important the work

that you do at home because in the end school can give you only the basics." He claimed that school was too theoretical and was not really stimulating, whereas when one studies on its own, one may find the stimulus to carry on and make progress. Nonetheless, he admitted that the role of formal education is still important. While one needs much self-commitment to advance, the school should give a foundation because learning on your own theory and practice is hard.

It is perhaps in this light that one should interpret results from the first survey (N=895), in which 40% of respondents stated that they learnt cyber security concepts and skills on their own. Even more revealing, of all CCIT participants (N=294) who had previously enrolled in a cyber security course, 47% declared that they had learnt cyber security knowledge and skills primarily on their own, while only 26% stated to have acquired these in class.

5.1.5 STEM competitions

Approximately half of the interviewees attended STEM competitions prior to the CCIT. Most students attended mathematics competitions, while a minority took part in IT and computer science events. Whereas students usually benefitted from attending, competitions role in shaping students' interest is unclear, if not limited. However, the initial difficulties students had when they approached these skills programmes help explain why they did not give up on their cyber security interest when they failed the CCIT admission test, as will be explored in section 8.2.

Students decided to attend STEM competitions mainly for two reasons: the desire to challenge themselves through a practical challenge and the willingness to be part of a team.

The excitement surrounding a skills event and the opportunity to practice what had been learnt in school was perhaps the primary reason students joined a STEM competition. One participant explained that he had always enjoyed a fun challenge because there "was nothing to lose for me." If he had won, he would have been content about the result, but there would have been no consequences if he had

not been able to advance. Another interviewee reflected that through these competitions he had wanted to challenge himself with a more practical activity than learning theory. He had been satisfied with his participation as he had put into practice some of what he had learnt, but also realized how much was there still to study. Another student reiterated this point, underlying that these challenges had allowed him to study deeper subjects that were not part of the school curriculum.

Another reason to attend STEM competitions was the willingness of some students to learn how to work in a team. One student noted that while the usual approach in these competitions is a division of labour, in reality, these competitions involved a lot of teamwork, where students could learn how to collaborate with peers. This is facilitated by a generally cooperative environment that does not discriminate or force newcomers to abandon the challenge if they are not as skilled as the other members. This was echoed by another interviewee who mentioned he was attracted by the idea of being part of a team composed of older students, who had taught him concepts and skills that he would have learnt only later on in the school year.

One interesting theme about participation in previous STEM competitions was that students perceived them as challenging endeavours, especially their first experiences.

One student revealed that these competitions could be demoralizing, especially when approached at a young age. He recalled his preparation for the computer science Olympics, where the educator had made him feel unqualified because he could not understand some of the concepts. He had gone back home in tears, and, at that moment, he was tempted to give everything up. His mother was key in his recovery process and told him to have faith in what he could achieve. He went on to win the school competition. Then, the competition moved on to the regional level, where he was unsuccessful, but he realized that “these things are difficult, I know it is normal to not understand, so I did not demoralize myself.”

A peer student had a similar experience, especially when he approached these competitions for the first time. He admitted that, in the first moments, he had been frustrated about his results because “I saw that other players had very high scores and so I was sad, but a little after [this sadness] was going away, and I restarted studying.”

In fact, despite the initial discouragement, students found the strength to carry on in their journey and started to see these competitions as opportunities to get better. They started to realize these events were not necessarily and always a challenge against someone or something, but rather self-improvement tools. The experience of one student explained it well:

> “Obviously, I did not obtain big results; however I was satisfied also because for each wrong answer (…) you have new hints that you can delve into. For example, if there is a cryptographic problem that I have no idea how to solve, perhaps at the end of the competition you go and inform yourself and you arrive at the next competition with more tools that are very useful for both the competition and for your professional future (…).”

This finding is important as it helps to put in perspective how students reacted to their failed admission to the CCIT training programme and why, notwithstanding that, their interest in cyber security did not falter (sections 7.1, 7.2 and 8.2).

5.1.6 Early professional exposure

Finally, this research sought to explore the extent to which early job experiences such as summer placements and internships impacted the development of students’ computer science interest. The main finding is that only one-third of students had some early professional exposure, and many seemed to downplay their experiences.

Only approximately one-third of students had some early approach to the professional world, and most of these experiences were in the form of the so-called

“Alternanza scuola-lavoro” (“school-work alternation”). This programme allows high school students to spend a limited amount of time, typically between one or two months during the summer, in a professional setting.

Examples of tasks interviewees were involved in included:

- Working in an IT-repair shop
- EU project in a Lithuanian web development company
- Visual Basic coding for a local company
- Coding in Python to manage servers in a local company
- Development of a web application for a local tribunal
- Redesign of a user interface for a local company
- Collaboration with an anti-mafia charity dedicated to repair and donate computers to families in need.
- Full-time work for an industrial engineering firm
- Management of a web radio
- Etc.

Although this did not seem the case for most interviewees, a summer IT placement helped at least one student understand this was the sector she wanted to be in. At the beginning, she did not imagine she was going to do “proper work,” but the IT manager of the firm made her accomplish several tasks, which even won the praise of the firm’s owner. She realized that many of her programs were going to be used by the company and helped her understand many practical tasks not taught in school. In addition, this experience had steered her towards computer science:

> “When I sat at the table and wrote down things that I liked or not, I realized that even that the school-work alternation (…) brought me to choose computer science, it really steered me.”

In reality, however, early professional exposure was not particularly instrumental to further develop students' interest, even among the one-third of students who had the chance to be briefly embedded in a work environment. Students, especially the high schoolers involved in the "Alternanza scuola lavoro" programme, tended to slightly downplay their experience. Despite enjoying it, they often concluded that their work had been limited.

For instance, one student went to work for a local firm that designed industrial automation software. She spent one month at the firm, where she felt she had been "the company mascot." Her tasks included checking and reviewing some Visual Basic programs. Her experience had been pleasant, but "in the end, it was rewriting old programs in a newer language. Yes, nothing exceptional, but I did it."

This finding seems to resonate with the results of the first survey (N=895), which showed that only a limited number of respondents (5%) had work experience in cyber security prior to enlisting in the CCIT (figure 15).

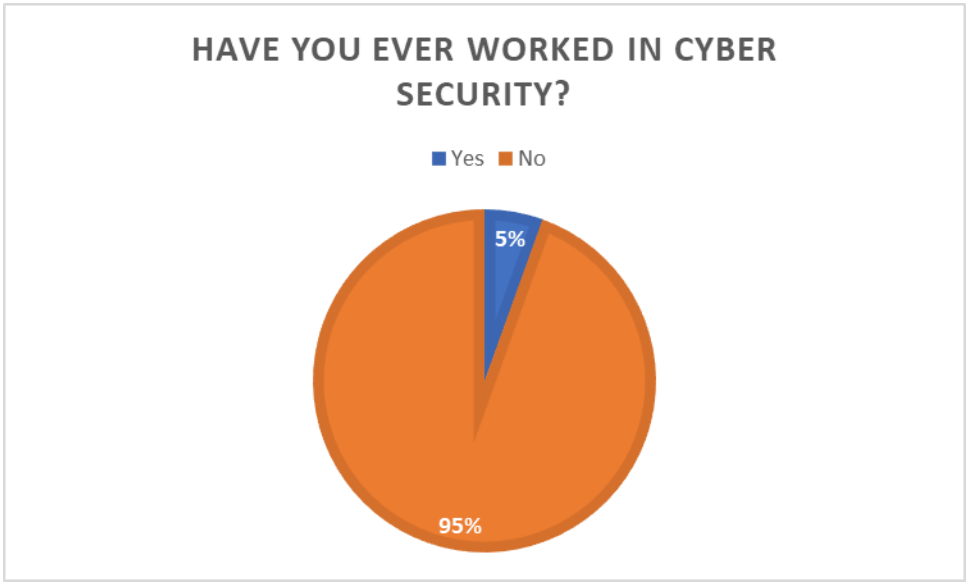

FIGURE 15

5.2 Cyber security interest formation in CCIT participants

The second part of this chapter identifies the most important triggers that made CCIT participants interested in cyber security. This section is central to the whole thesis as it helps understand what factors can be used, in isolation or in combination with each other, to create a system of incentives that might increase the pipeline of cyber security professionals. The establishment of a "cyber security interest development system" will be discussed in chapter 10.

Data from the second survey (N=390) provided a good overview of the elements contributing to cyber security interest among CCIT participants (figure 16). The quantitative nature of these data makes these factors rankable:[31]

1. Curiosity (60.3%)
2. Formal coursework (42.8%)
3. The CCIT (36.2%)
4. Encouragement coming from a professor (25.6%)
5. TV shows (20.5%)
6. Reading technical documentation (14.1%)
7. Capture the Flag competitions (13.6%)
8. Friends and family (13.1%)
9. Victim of cyber crime (1.5%)
10. Other (1,5%)
11. Not interested in cyber security (1.3%)

[31] The survey question allowed respondents to choose up to two factors. This is why percentages do not add up to 100%.

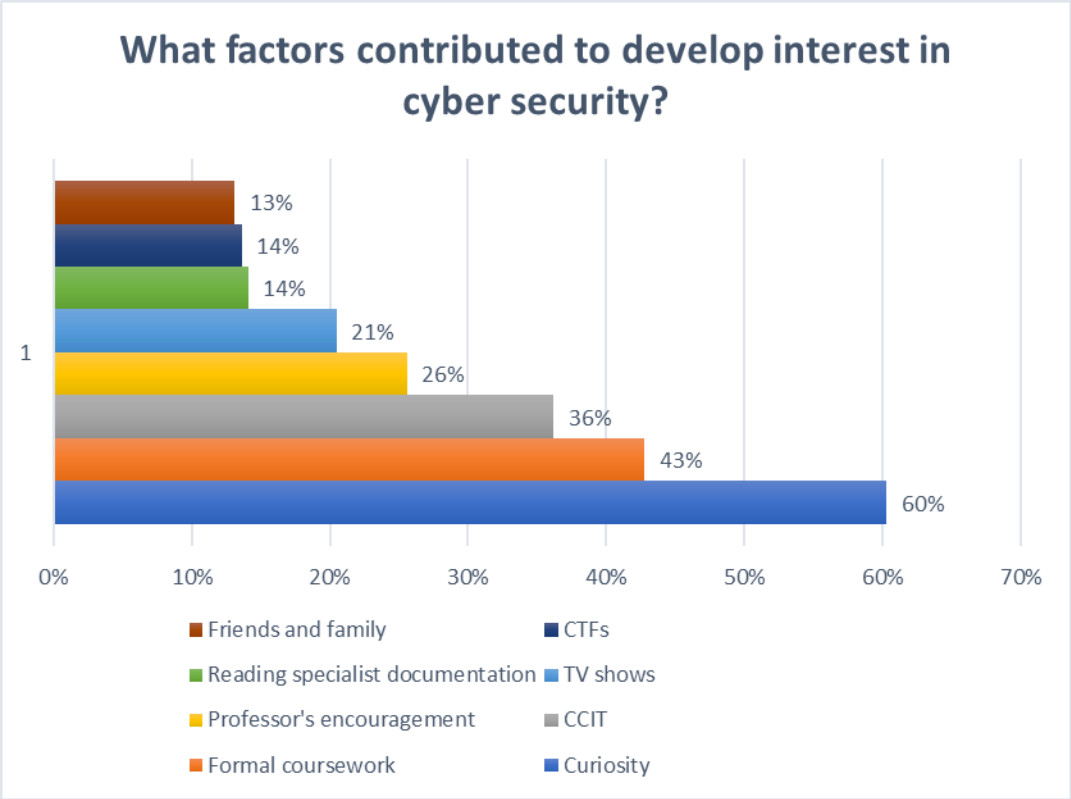

FIGURE 16

Interview results were broadly in line with those of the survey and had the benefits of providing deeper insights on how the above factors shaped the formation of cyber security interest. Notably, the interviews made it clear that no single dominant explanation described how participants became interested in cyber security. Most often, it was a combination of these factors that contributed to forming participants' cyber security interest.

5.2.1 Curiosity, internet browsing and readings

Approximately one-third of study participants came to cyber security quite randomly, such as through internet browsing or social media. Once their attention and curiosity had been captured, some of them started to develop a more active interest in the topic. Other students found news of data theft online, which spurred

them to be generally more alert when downloading content online. At times, curiosity made them watch videos or read technical documents and books.

For example, one student started watching YouTube videos, and from then on, his cyber security interest increased:

> "out of curiosity…because when I was a kid, I could not understand how a computer worked, what were the related security issues and what could compromise its security. Thus, I started to get more into cyber security, and interest followed. (…) From then on, I have become more and more interested, until I started reading cyber security technical documents by myself…It was not because of any education requirement, I was only curious."

Another student started reading books on network security, reverse engineering and cryptography when he was 15-16 years old. He started reading these books not because they were assigned in school but because he was curious. He started with popular science books and then more scientific and mathematical books. He said that it was through cryptography that he had become interested in cyber security: "because I am a shy person and I like to keep many things about me secret. So, I have always seen in cryptography an extra layer of protection."

5.2.2 Coursework and conferences

Approximately one-third of interviewees started to develop an interest in cyber security due to some sort of academic endeavours or venues, though not necessarily through formal education.

This finding is in line with survey results (figure 17) which showed that formal coursework was the factor with the second-highest percentage (43%) after general curiosity (60%). This result is reinforced by another result from the first survey (N=895), which found that 30% of respondents had enrolled in a cyber security course, either on-site or online, before signing up to the CCIT.

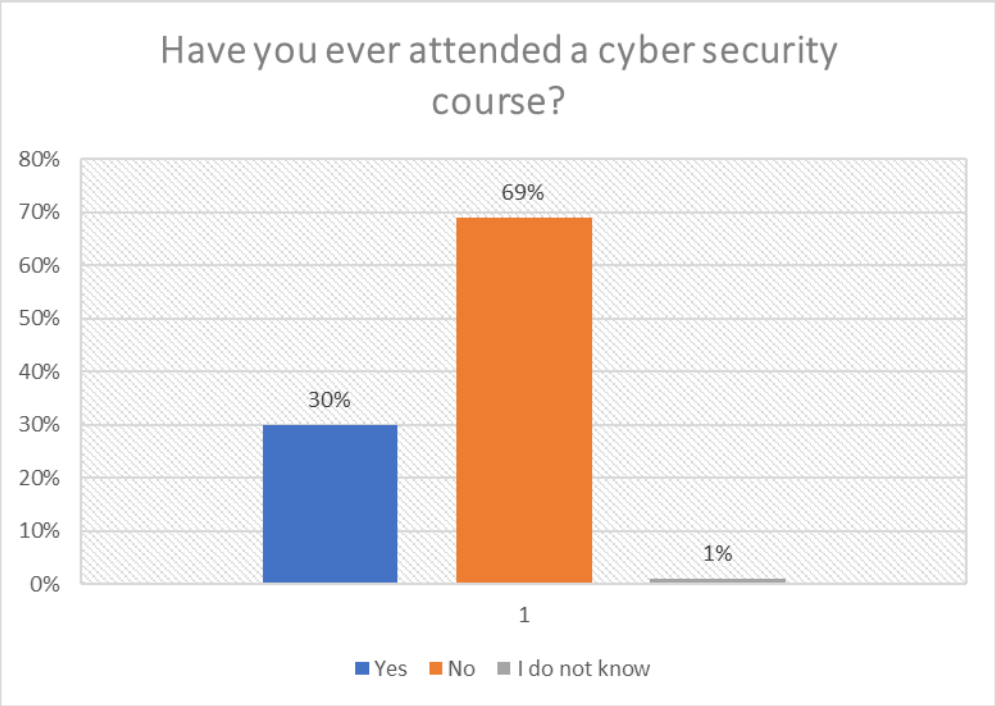

FIGURE 17

Some students developed an interest in cyber security through regular mandatory coursework, either in high school or university. For example, one student studied cryptography in his last high school year. The course was stimulating and made him want to deepen his acquired knowledge through algorithm testing.

Another student who had studied cryptography while at university thought it was an exciting subject, which made him realize how vast cyber security was and the extent to which it could offer many diverse opportunities. He characterized cyber security as a very “cross” subject and with much variety.

Two students had their interest in cyber security even more profoundly shaped by their formal education. At the time of interviews, they were both enrolled in master’s degrees, one in computer science-engineering and one in cyber security.

The computer science-engineering student became enthralled by cyber security from the first introductory lesson in the course Computer Security 1, when he had started liking the topic “as a field, as a reasoning tool, as a world on its own.” He loved it because cyber security was complementary to what he already knew about computer science and found that the class had helped find information that could only be gathered after long online searches. He would not have discovered this world without this university course.

The other student, who was enrolled in a cyber security master’s degree, opted for such a graduate programme because he realized it was the field he was most attracted to during his bachelor's degree. He thought cyber security was interesting “because of its 3,000 different perspectives.” During his graduate degree, he had followed several exciting courses, including network security, malware analysis, penetration testing and ethical hacking, and asserted that:

> “I have started to experience the real cyber security through this master’s degree.”

However, it is not only through formalized education that students started forming an interest in cyber security. Some had the chance to get deeper into it through courses offered by private entities, online courses, and thematic conferences.

For example, a student enrolled in a 300-hour course provided by a cyber security company in Milan. The course allowed him to understand cyber security more holistically, mainly because non-technical topics such as policy and law, crisis management operations and other similar courses were taught in class.

Another student used online courses to reach a rounder understanding of cyber security. During the first year of his computer science degree, he bought several online courses on Udemy,[32] where he learnt basic cyber security concepts such as fake handshakes and how to connect to networks with low-level security.

[32] Udemy is a massive open online course provider aimed at professional adults and students.

Some students became interested in cyber security due to school or academic conferences. One student explained that her high school used to organize conferences where computer science experts were invited to talk about security and other “flashy topics to get the attention of teenagers.” These conferences had prompted her to do some extra readings on security incidents, trying to gauge how the security team involved in the crisis management had dealt with them. Another student once attended a conference because his professor was there to deliver a talk. The conference was an excellent experience, as he met various cyber security experts and learnt more about the field and the industry. There, he realized the “incredible” demand for cyber security experts.

5.2.3 The CCIT

Approximately one-third of interviewees stated that the CCIT had sparked their interest in cyber security. Some students candidly admitted that they had never really thought of cyber security before realising there was a national skills competition centred on it. The CCIT made participants aware of the topic, which otherwise would have remained unknown.

A student explained thoroughly the process through which cyber security had been put on his radar by the CCIT. He recalled that his university had sent an email describing the possibility of enrolling in a cyber security course (i.e. the CCIT). After a quick internet search, he thought it could have been an interesting opportunity and signed up. I asked him to what extent he was interested in cyber security beforehand, and he revealed that he had always been interested in computer science, especially programming, but “the world of cyber security, I did not know it existed…I did not have any contact with this world.”

Another participant explained that:

> “Well, my interest in cyber security was switched on by this competition…if I am interested in cyber security, it is because of this competition... [if it was not for it], I do not think I would have looked into it.”

Similarly, a student declared that he had never looked into cyber security until he received information about the CCIT: "…I had not heard about it (cyber security), perhaps mentioned it a bit randomly in my last year of high school when we started doing a bit of theory. But for the rest, nothing, before that moment, zero."

This finding is important as this research did not originally hypothesize that the CCIT could be among the factors triggering initial interest in cyber security interest. The result gives the CCIT an additional value as a policy to mitigate the cyber security skills shortage as it reveals the potential role of a NCSSC to initiate interest rather than only influencing it. The implications of this finding are discussed in chapter 9.

5.2.4 Cyber security skills competitions

Approximately 20% of interviewees became more familiar with cyber security by participating in other cyber security skills competitions before the CCIT.

This result is in line with results as shown by figure 18 and another survey question (N=895), which asked CCIT participants whether they had ever attended a cyber security skills competition before signing up to the CCIT: 22% attended at least one.

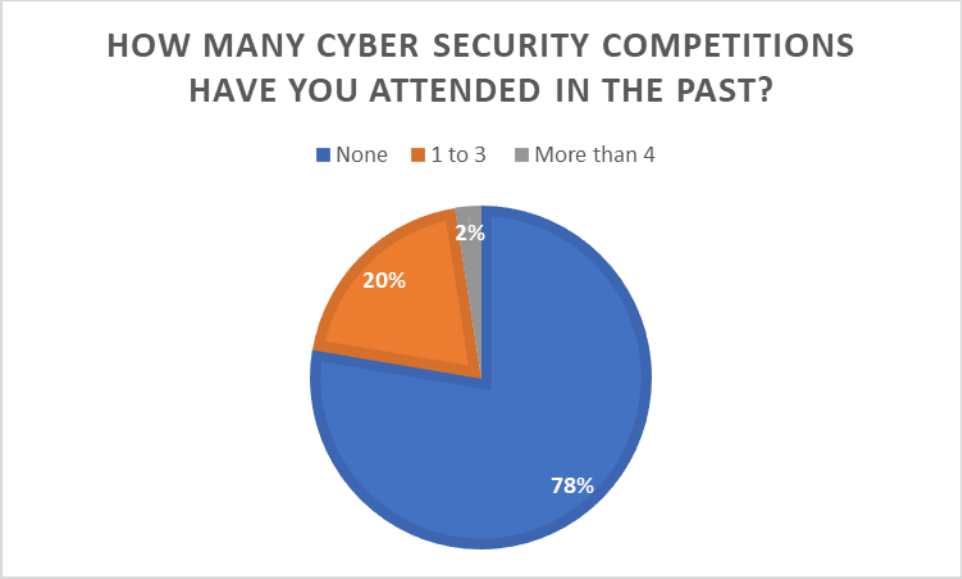

FIGURE 18

For example, one student attended three official cyber security skills competitions before the CCIT. Moreover, he had also been practising online through archived competitions, which organisers had made available to enable participants to complete them at their own pace.

Another interviewee stated that one of the most exciting aspects of cyber security was that "it is possible to do various online trainings that are more like games." These games (i.e. skills competitions) allow those participating to understand how systems can be compromised and manage vulnerabilities. He felt this was fascinating because, while these competitions are not conceived as professional training, they help people understand very "valuable aspects."

An interesting finding that mirrors what was previously discovered about participation in STEM competitions (section 5.1.5) is that even those students who attended cyber security skills competitions thought that their first experiences had been harrowing because of the high-level skills required. Nonetheless, the initial

difficulties did not convince them to abandon their interest; instead, they fuelled their desire to learn more and advance their knowledge.

One student had attended five competitions with his university team before attempting the CCIT and felt that, as a self-described “amateur,” he did not achieve anything noteworthy. He believed his contribution to his team so far had been minimal. He explained that achieving competency in cyber security is extremely difficult, and before one can make a significant contribution, it takes a lot of effort and time.

Another student admitted that the first cyber security skills competitions had gone “very badly,” which had made him realize how unprepared his team was. Despite being upset, however, after the negative competition outcome, there was a reaction:

> “something comes that pushes you to continue studying and to say, damn, it is not possible I can’t do these things, and so, let’s say, the willingness to learn emerges, your curiosity increases, to find new sources (of information) and increase this knowledge.”

This experience was similar to the one of a peer who characterized as “very frustrating” his first skills competition. This, however, had pushed him even more: “The bigger the frustration, the more I was pushed not to give up,” suggesting that the more unsuccessful he was, the more he wanted to learn and improve to get a better score the next time.

As for the finding on generic STEM competitions, this finding is important as it anticipates and helps explain why students did not give up on cyber security after failure to be admitted to the CCIT.

5.2.5 Key figures

Interviewees mentioned key figures such as professors and friends as relevant factors that introduced them to cyber security. Moreover, some students reflected upon the role that TV shows like Mr Robot[33] had in stimulating their thinking about cyber security.

The role that people such as professors and friends was relevant for some participants. One student spoke highly of his "famous" cyber security professor, "whom, I think, has motivated everyone in the [cyber security] group to go down the cyber security path." His professor was key in developing cyber security interest because of how professional he had been with him and the rest of the students in the university security group, which the student joined following his suggestion.

Another student had a group of friends with whom he discussed computer science problems. The "team" was composed of a school friend and other members from all over Italy, whom he had met online. Similarly, another study participant had a friend who shared a common, although complementary, computer science passion. He was more interested in developing websites, whereas his friend had some knowledge of cyber security topics such as backdoors and keyloggers. When they started talking about cyber security: "I understood that this was cool, I mean, I was inspired…I liked it. Then, I saw the CCIT, and I asked him if he wanted to come along…he said yes, and we enrolled."

For other students, TV shows like *Mr Robot* had a role in arousing them and pushing them towards cyber security. One student said that he saw hackers and other experts that work in the sector:

[33] Mr. Robot is an American TV show staring Rami Malek as Elliot Alderson, a cybersecurity engineer and hacker who is recruited by an anarchist group to destroy all debt records by encrypting the financial data of E Corp, the largest conglomerate in the world. The TV show won numerous awards, including two Golden Globe Awards and two Primetime Emmy Awards (Wikipedia, n.d.).

> “like a dream, an objective to achieve…I saw it this way, and I saw it like a dream. I wanted to know how they worked, what they really do, how to get there.”

He said that he liked *Mr Robot* for the direction and enjoyed all components of the security focus. He particularly enjoyed the main character, Eliot, who “without any big help, in a poorly equipped garage, (…) was able to unsettle the entire world, something very powerful.”

Likewise, another student suggested that *Mr Robot* was among the reasons he chose to enrol in a computer science degree, which reignited his interest in cyber security and influenced his university choice.

5.2.6 Malware and cyber crime

Approximately 15% of interviewees were inspired to get deeper into cyber security because they sought protection from cyber criminals. Some students wanted to add an extra layer of protection to their online activities, whilst others were victims of data theft.

For example, one student advanced the view that, while no particular moment in his life had led him to cyber security, he had become aware that the internet and networks are increasingly pervasive and, consequently, there is the need to make them secure. Hence, he became more interested in security for practical reasons, including himself online.

A couple of interviewees, however, had much closer encounters with the dark side of the IT world, when they, or a family member, had become the victim of cybercrime:

> “I started to get interested in cyber security after my Gmail account was stolen. I would like to help other people that face these situations. They are very awful.”

Within his family, he was not the only person who had fallen prey of cyber criminals, as his mother also had her email credentials stolen. When his data were taken, he admitted that information in his email account was mainly related to games, which he labelled as "trifles…I do not even want to imagine what would happen to big corporations." He had his question answered when his mother's data were stolen. As her computer stored sensitive work data, they had to report the theft to the police. In the end, these episodes pushed him to become more involved in cyber security.

Similarly, another student developed an interest when his mother could not connect to the internet because malware had infected her laptop. After the incident, he decided to deepen his knowledge and go on various antivirus blogs. On a different occasion, he had to eliminate a Loki[34] from a colleague's phone, which it was one of the most challenging tasks he had ever accomplished:

> "When you try to eliminate it, the Loki transforms into a ransomware and could block the entire phone. The only way to expel it from the system was to enter in safe mode and inject some strings…I remember it was hard. I had to look up for code on the internet because I did not know about it. This episode, rather than discouraging me, developed my passion for cyber security even more."

Another student did not become a victim of cyber crime but instead engaged in a "potential" online criminal activity. She and her group of friends created a phishing website to steal the login credentials of a peer student who was using a fake social media account for dubious purposes. Nonetheless, this activity was only *potentially* criminal as she and her friends never launched the website. In reality, they were all aware they were attempting to do the opposite of what one would do in cybersecurity, but she added they were doing it for amusement. It was more like a group project rather than anything aimed at something criminal: "We gathered, and we agreed to create this website and to make it look similar to the Instagram login page…We put up a little server on a friend's computer, and we created this

[34] A Loki is an info stealer malware that can steal credentials, disable notifications, intercept communications and exfiltrate data (Trend Micro, 2019).

website…We tested whether it was working, and it was working fine. Obviously, we did not use it, the aim was to do it for fun…And well, it was fun."

5.3 Summary of findings

Chapter 5 had the objective of identifying the main factors that contributed to developing cyber security interest among participants before the CCIT. In order to better understand the overall context where interest in cyber security flourished, it also dug deeper into the origins of students' interest in technology and computer science. The findings of this chapter are helpful to contextualize chapter 6, which establishes a baseline of participants' cyber security interest before attending the CCIT. Moreover, it provides the evidence required to discuss the creation of a system of interest formation with the goal to generate a national pipeline of cyber security professionals (ch. 9).

Section 5.1 showed that study participants started to use a computer at a young age, generally between four and ten years old. Their journey into computing mainly started through video gaming or school computer usage. Another critical aspect was access to IT tools, namely computers and laptops that parents used to perform their jobs with.

While video gaming and school activities pushed students to get closer to technology, many interviewees had the desire to understand more deeply how systems, networks, and data worked. This led them to delve into computer science and develop related knowledge and skills. Over the years, study participants used ICT technology for purposes that would not distinguish them from other young users, such as entertainment and school activities. However, they differentiated themselves by learning to code and attempting various forms of IT experimentations.

While approximately one-third of interviewees was directly or indirectly influenced by family members in their choice to pursue computer science, most interviewees developed an interest in IT independently from them. Interview data are

corroborated by survey results, which showed that less than 20% of CCIT participants' parents had studied an IT-related discipline or had worked in the IT sector. Regardless of these direct or indirect influences, however, a solid finding is that CCIT participants were supported by their families in their choice to pursue an IT career.

Most CCIT participants were enrolled in IT-specific secondary education schools and degrees, and one can argue that their passion for computer science (and STEM subjects more broadly) drove their educational decisions. This appears to suggest that education was not the primary cause of their interest in technology and computers. In fact, around 40% of interviewees were dissatisfied with formal schooling, which prompted them to do extra work at home and delve deeper into concepts not taught in class. These results are in line with what was found by the first survey, in which 40% of respondents said that they had acquired cyber security knowledge and skills primarily on their own.

Approximately half of the interviewees attended STEM competitions such as computer science and mathematics Olympics before the CCIT. While they usually listed several benefits in taking part, the impact of these competitions on their interest development seems minimal. Those who attended noted that competitions were challenging due to the high-level skills required, but after the initial discouragement from early negative results, they started to see competitions as self-improvement opportunities.

Finally, interviews showed that only a third of students had some early professional exposure in the form of short summer internships, but many tended to downplay their experiences. Therefore, it can be argued that the impact of these early professional placements did not significantly affect students' computer science interest.

To summarize, one can argue that the following factors seemed to be particularly important in explaining early interest in technology and computer science among CCIT participants:

- Gaming
- School activities involving IT
- Desire to understand how a computer works inside
- Parental support to pursue computer science
- Programming and experimentation
- Self-learning

Section 5.2 used survey and interview results to identify the primary triggers that elicited students' interest in cyber security. The three main elements were:

- General curiosity in the topic
- Formal and informal coursework
- The CCIT

Most students seemed to have heard about cyber security for the first time through internet searches and social media. Once headlines captured their attention, students would often start reading more technical documentation in online blogs or specialized books.

Coursework was also an essential factor that triggered students' cyber security interest. The most typical form of coursework was usually a mandatory course that was part of the high school or university curriculum. Other informal educational activities included online courses, training provided by private companies and conferences.

Another important finding of this section is that the CCIT is among the most cited factors by students explaining how they became attracted to cyber security. Interviewees explained that cyber security was obscure to them before finding out about the competition. This is a significant result, which adds an important dimension to the CCIT as a policy to mitigate the cyber security skills shortage, which will be discussed in chapter 9.

Other factors were highlighted by the survey and interviews, even though they were generally less popular. Some students approached cyber security through skills competitions, even though their first experiences were problematic because

they required high-level skills. Similarly to findings related to STEM competitions, though, these first obstacles proved to be motives for further learning.

Students also developed an attraction for cyber security thanks to key figures in their lives. “Real” figures included professors and friends, who introduced them to cyber security in the context of mutual interest for technology and computer science. Fictional figures such as *Mr Robot* also played a role in intriguing CCIT participants.

Finally, some students became interested in cyber security after they had been victims of cyber crime or someone else close to them. As students realized the perils of our reliance on IT systems, they desired to help people who fall prey to the dark side of cyber security.

6. An assessment of cyber security interest before the CCIT

Chapter 6 has the objective of assessing the cyber security interest level of CCIT participants before the beginning of the skills competition.

Establishing a baseline is an essential first step to understanding how the CCIT influenced cyber security interest, which is the goal of chapter 7. In fact, knowing the interest level of participants before the competition allows us to more clearly gauge the extent to which their interest evolved thanks to a before-and-after assessment.

Cyber security interest is divided into interest in cyber security as a topic and as a career. This is helpful to examine whether participants differentiate between the two and whether the CCIT could influence only one outcome variable or both at the same time.

This chapter is organized into three main sections:

- Section 6.1 assesses interest in cyber security as a topic
- Section 6.2 evaluates interest in cyber security as a career
- Section 6.3 summarizes the findings of this chapter

6.1 Interest in cyber security as a topic

Interest in cyber security as a topic was high among most students before the start of the CCIT, and this finding is backed by survey and interview data. They manifested their interest by routinely performing cyber security tasks and independently accessing related information. However, interest was not high for everyone. While those indifferent to cyber security constituted a minority, this finding is relevant as it anticipates the theme of "competing interests," which will be presented in chapter 7.

Results from the first survey (N=895) overwhelmingly confirmed that the individuals who signed up to the CCIT were already interested or very interested in cyber security before the competition (figure 19):

- 52% of respondents strongly agreed with the statement, “I am interested in cyber security, and I would like to increase cyber security knowledge and skills”;
- 28% and 11% respectively agreed or somewhat agreed with it. This means that 91% of respondents were interested in cyber security as a topic before the CCIT started;
- Only 5% of respondents were neutral, and only 4% disagreed with the statement.

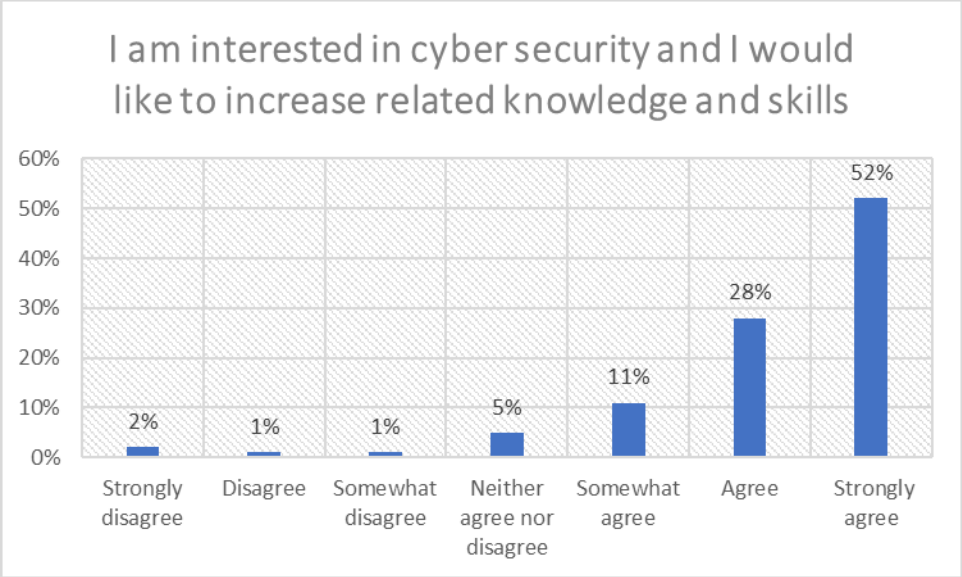

FIGURE 19

Moreover, 80% of survey respondents agreed with the statement “I would like to enrol in a specialized course that would help me access the cyber security sector;” 11% were neutral, and 9% disagreed with it (figure 20).

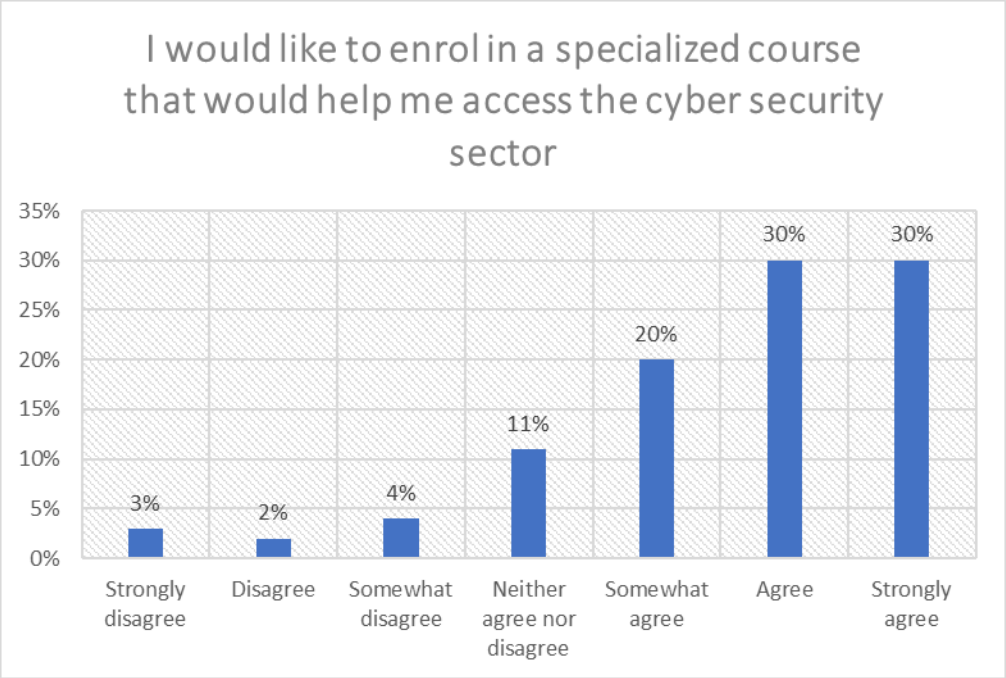

FIGURE 20

Survey data were useful to gauge whether interest was present but could not describe how developed this interest was. Therefore, interviews were used to gain a deeper appreciation of participants' cyber security interest, particularly the relationship between feelings, value and knowledge. When this was possible, interviews attempted to assess how frequently, voluntarily, independently, and with what level of knowledge participants were interacting with cyber security content, as Hidi and Renninger (2016) suggested.

Interview data confirmed the findings of the survey. Indeed, most interviewees (>80%) declared to be interested or very interested in cyber security as a topic. I asked participants to quantify and compare this interest to another interest they might have for other topics and subjects on a 10-point scale.

For example, one interviewee said that "I would give it something between 8 and 9 because it is a very interesting topic. It is very attractive…". Another participant would give his interest in mathematics a score of 8 and 9 to cyber security, although he acknowledged that these are complementary topics, and one needs

to have a strong mathematics foundation to operate well within the computer science field. Some students showed even higher interest levels in cyber security, which had surpassed interest in other topics such as computer science ("Let's say that if I give computer science a score of 8, I could give a 9 to cyber security. I am quite interested in it") or mathematics ("I would give it a 10, I am very interested – *(Researcher) Is it at the same level as mathematics?* – Even more, actually").

To understand the "depth" of interest in cyber security as a topic and what participants meant by it, I asked them to give concrete examples. Some students expressed interest through the routine performance of cyber security-related activities, which showed their commitment and attraction to what they saw, most of the time, as a new and exciting topic worthy of further exploration.

For instance, one student undertook cyber security activities independently of what was assigned in school. For example, one day, he downloaded on its own Wireshark, a network protocol analyser, to understand how it worked. Another student started and continued to perform antivirus scanning and in-depth computer optimizations after receiving a Kaspersky's antivirus subscription. He became interested in the software's security reports: "my first experiences came from there, I was trying to understand why I could not access a website, what the software had found, what would happen if I did not quarantine the file." Later, he learnt how to fix his computer by removing malware properly, and his family and friends took him for "a little computer specialist."

Another student performed "very rudimentary, but fun penetration tests," creating websites and then attempting to penetrate them. Similarly, another student performed "laboratory tests" for one or two hours a day in his bedroom using Raspberry Pi[35] and various versions of Linux. He said he thinks in "cyber security

[35] Raspberrry Pi is a series of small single board computers developed in the UK by the Raspberry Foundation.

terms, namely what can be called the programming method, in algorithms…my mind now thinks in algorithms."

The above are just a few examples of how students with medium to high interest usually expressed their attraction to cyber security. However, some interviewees had already developed a more substantial interest and commitment, which was apparent, for example, from their enrolment in cyber security courses and degrees or participation in security skills competitions. These examples have been described already in section 5.2, which explains the processes and factors that contributed to the formation of cyber security interest in CCIT students.

While this positive sentiment towards cyber security as a topic was widespread among interviewees and survey respondents, it was surprising to find some of them to be almost utterly unattracted to cyber security. This result was unexpected as one would imagine participants who had voluntarily signed up to a cyber security skills competition to show some interest in the topic.

Survey results (N=895) found that a minority of respondents (4%) was uninterested in cybersecurity and unwilling to develop related knowledge and skills (figure 20, pg. 169).

Interview data reflected this finding, with four students equally split between CG and TG, who declared to be only somewhat interested or not interested at all in cyber security.

This lack of interest was sometimes due to the fact that students had signed up to the CCIT with the primary goal of challenging themselves through the admission process rather than interest in cyber security. For instance, one student admitted that he had signed up online "almost by chance" and that he had been more interested in the programming side of the admission test.

Another important reason was that cyber security seemed to be "vying for influence" among other topics, which meant that, very simply put, for some

participants cyber security was not their preferred choice in the realm of computer science subjects. For example, two interviewees candidly expressed that:

> "I am not interested because I have bigger interests in other areas. Not necessarily because I do not like cyber security, but because I have other passions that bring me towards different sectors."
>
> "As a study topic, [cyber security] does not interest me that much, I am more interested in subjects like theoretical computer science and formal methods. However, it interests me as a competition, a fun activity."

Although only a minority of interviewees and survey respondents were almost entirely uninterested in cyber security, this result should not be underestimated. In fact, this finding is crucial as it anticipates the theme of "competing interests," namely how interests in different topics and careers can coexist with one another and thus have an essential bearing on NCSSCs' ability to influence students' interest and key educational and career choices. Results on this topic are presented in section 7.5 and analysed in chapter 9.

6.2 Interest in cyber security as a career

Both qualitative and quantitative results confirmed that most CCIT participants had at least thought of becoming cyber security professionals one day. Survey results, however, showed an interesting discrepancy between interest in cyber security as a topic and as a career, suggesting that students distinguish between the two. Moreover, similar to the results above, a minority of students were reluctant to consider a career in the sector.

The first survey (N=895) showed that the individuals who signed up to the CCIT were broadly interested in a cyber security career. Indeed, 78% of respondents at least somewhat agreed with the statement "I would like to have a career in cyber security," whereas 9% had adverse feelings towards such a prospect (figure 21).

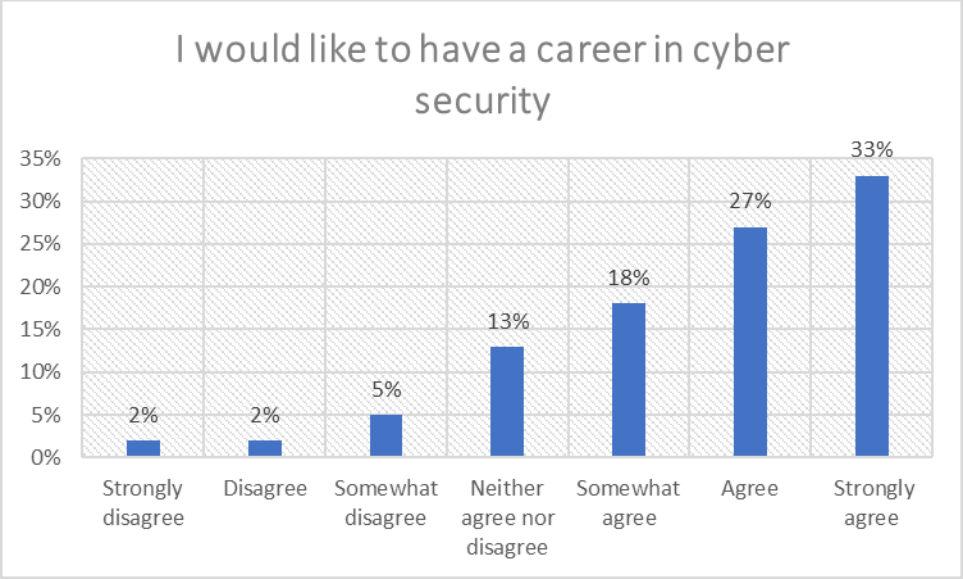

FIGURE 21

Furthermore, 68% at least somewhat agreed with the statement "I will apply to cyber security positions at the end of my studies;" 19% had neutral feelings, whereas 14% of respondents at least somewhat disagreed with it (figure 22)

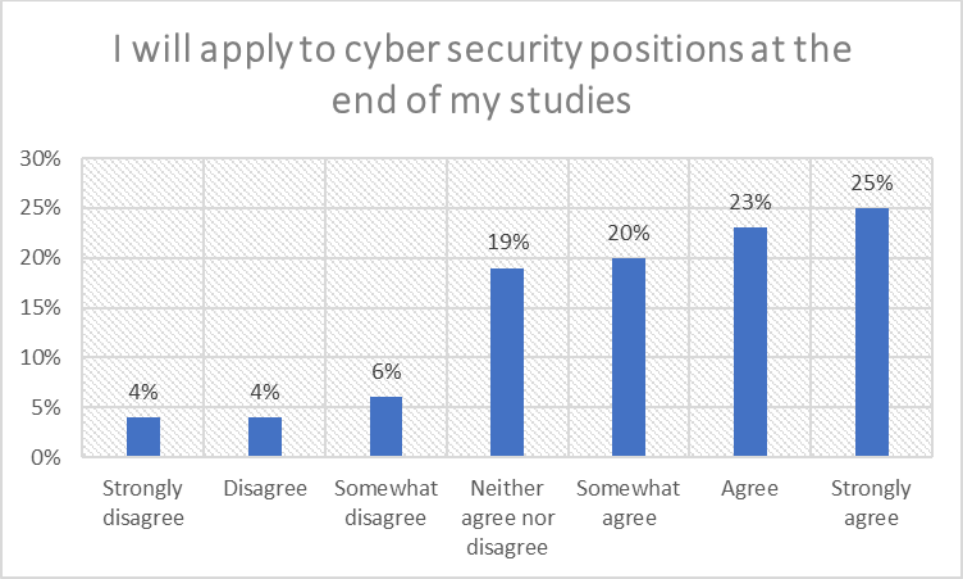

FIGURE 22

Finally, 81% of respondents at least somewhat agreed with the statement “I would like a successful career in cyber security and make an important contribution to the sector,” compared to 9% of survey respondents being somehow less inclined; 10% neither agreed nor disagreed (figure 23).

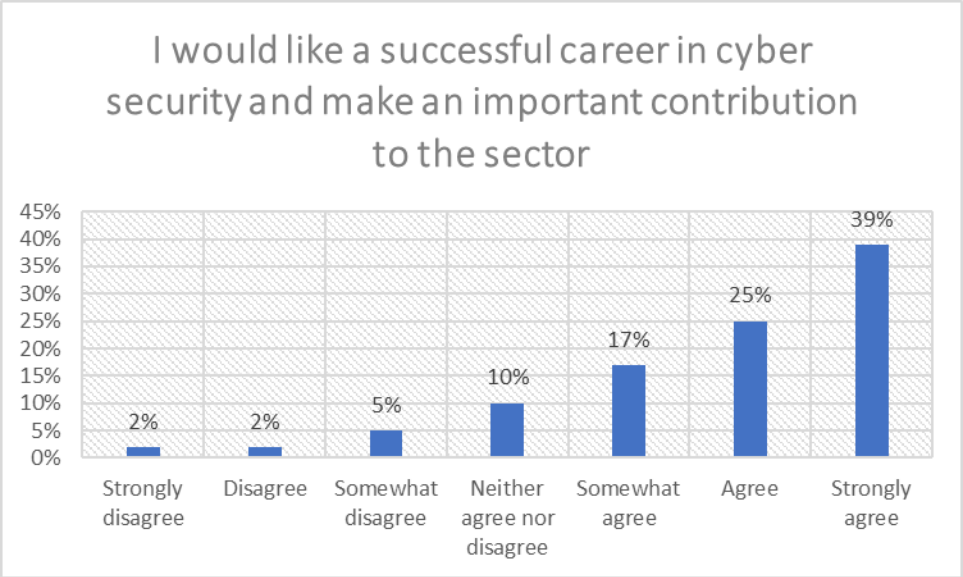

FIGURE 23

An interesting finding that emerged from comparing these data with those in the previous section is that CCIT participants seemed to be more interested in cyber security as a topic than as a career.

Data on the statement “I am interested in cyber security, and I would like to increase related knowledge and skills” showed that 91% of individuals had a positive sentiment towards it, including 52% who strongly agreed. If one averages the results of the three statements in this section, “only” 77% of respondents seemed inclined to a cyber security career. More formally, interest in cyber security

as a topic was largely but not perfectly correlated[36] with interest in cyber security as a career:

TABLE 14 CORRELATIONS BETWEEN CYBER SECURITY TOPIC AND CAREER INTEREST

	I would like to have a career in the cyber security sector	I will apply to jobs in the cyber security positions at the end of my studies	I would like a successful career in cyber security and make an important contribution to the sector
I am interested in cyber security and I would like to increase related knowledge and skills	r=.686	r=.551	r=.625
N	895	892	893
	Correlation is significant at the 0.01 level (2-tailed)		

Although these results were still within a framework of clear acceptance of a cyber security career in principle, they also suggested that students could differentiate between interest in cyber security as a topic and as a choice of profession. Theoretically, it could be possible for the CCIT to influence only one of the two variables rather than both. The implications for a NCSSC as a skills shortage policy are discussed in chapter 9.

The interviews gave more context to these results, explaining how and why CCIT participants viewed cyber security careers positively, but also why some of them

[36] Using Pearson correlation

were reluctant, if not totally unwilling, to embrace the prospect of a cyber security job.

Most interviewees were generally attracted by the idea of becoming cyber security professionals, even when compared to other IT professions and domains. A student from the CG gave her cyber security career interest a score of 8/9 out of 10. While she believed that most cyber security jobs were interesting, there were some she was particularly fond of, for example, the forensic expert:

> "(it is) very interesting, I like watching TV shows like Chicago Med. It is very interesting to analyse events, investigate what happened, pursue the criminal who committed an online crime, who stole pictures, and trace back the crime to a person."

She knew about cyber security roles because her high school professor had once mentioned them when discussing what jobs one could have in the IT field. As of now, she would prefer a cyber security job even over her other great passion, programming. She thought that cyber security "would be a very cool job, also because it is done by few, especially few women…it is something that attracts me even more, being among the first to do it, it would be very cool."

Another student pursuing a master's degree in computer science-engineering with a strong focus on security said he was attracted to almost all cyber security jobs. He knew of various roles as he had already attended some cyber security conferences, where he had befriended some professionals and asked them about the sector. He had also taken part in some initiatives organized by the university's career service, where various cyber security experts had come to give presentations on job opportunities. Overall, he thought to know what jobs were in demand in the labour market.

Another participant was interested in blending cyber security with computer vision and facial recognition. He claimed that the computer vision sector is developing and expanding, requiring a critical security component. He gave the example of deep fakes, saying that algorithms testing whether a video has been altered will

be increasingly warranted. He believed that a career in cyber security could be rewarding because of the impact one can have as a professional:

> "In cyber security, you have an impact because you work to avoid that your company loses money, you are defending a system, you are protecting people, data…so, you have an impact. The public does not notice this work because they take it for granted that the application is supposed to perform in a certain way, but in reality, you have a huge impact…I do not seek the approval of the common user, but having this sort of impact is satisfying."

While many students showed interest in a cyber security career without being overly specific about their future educational and professional plans (see section 7.3 on career decision-making difficulties), a limited number of students instead showed off very clear and ambitious plans. For example, one student from the CG declared:

> "I will go to MIT in Massachusetts to do a master's degree and a PhD in cyber security."

This student aspired to go to MIT because he claimed it was the world's best computer science university. If MIT did not work for him, he had identified Caltech, in California, as an alternative. His career plan included first pursuing a bachelor's degree at La Sapienza University in Rome because "it is highly ranked" and a well-known computer science department in Italy. He gave his cyber security career interest a maximum score of 10, even above his other great passion, systems engineering, which he saw as profoundly intertwined and "correlated" with cyber security.

Nonetheless, almost 20% of interviewees were only mildly or not interested at all in a cyber security profession. Explanations for their reluctance included general uncertainty regarding the future, lack of knowledge on cyber security roles and other competing interests.

One high school student from the control group, who probably had the most eclectic profile among those interviewed, is illustrative of the logic of competing interests, which will be further explored in section 7.5. Despite being interested in computer science and programming, he had very different aspirations, namely enrolling in a bachelor's degree in economics and studying subjects such as international economy and relations. I asked him if he had ever thought of combining his interest in computer science and the social sciences, and he concluded that computer science "will always be there" and that he would keep it as a hobby because perhaps "it will give me more satisfying moments later on." He did not wholly exclude becoming a cyber security professional one day. He knew that cyber security experts are in high demand, and he thinks one would be able to find a stable and well-paid job, but remains highly sceptical: "The ways of the Lord are infinite…it depends…but I would say no…it is not that I do not want to do it, but it is difficult, it is very difficult for the competencies that one needs and that I do not possess."

Three students from the treatment group were quite categorical in excluding the possibility of becoming cyber security professionals one day.

One student answered an uncompromising "no" when I asked whether he had ever considered working in cyber security. Instead, he preferred a career in artificial intelligence: he gave a score of 6 to his cyber security career interest and 9 to artificial intelligence.

Another student was also blunt about the possibility of joining the ranks of the cyber security workforce. As much as he did not find cyber security interesting as a study subject, he was also not attracted by a career in cyber security. This option had once been presented to him by a professor during a career coaching session:

> "One day, one professor asked whether I was interested in becoming a national security professional. I thought about it, it was intriguing, but I am more interested in other careers."

Finally, one student said he would discard the possibility to become a cyber security worker, suggesting he knew too little about cyber security to go for it:

> "I must be honest, I know so little about cyber security that I will never pursue a degree in it. (…) I do not know what kind of professional roles exist, in what sector, where they work, I cannot tell."

When planning his professional career, he had two criteria: finding a job and having a good salary. Both engineering and medical schools met these criteria. He was more inclined to go to medical school because his parents are both doctors, and he saw it as something "familiar," something he was not afraid of, because "medical school in Italy is a straight line, something very certain." To conclude, he gave a 5 to his cyber security career interest and 9 to become a doctor.

6.2.2 The dream cyber security job: the penetration tester

If one must nominate a single cyber security job role that students seemed to be attracted the most to, it was the penetration tester.[37]

An open-ended question of the second survey asked students what cyber security role they were more interested in, and approximately 35% of respondents answered the penetration tester as the most intriguing.

Interviews reiterated this finding and helped comprehend why students seemed so fascinated by this role. For instance, one student did not know "where, how and when," but one day, he said, he would become a pentester because he is "a fan." What intrigued him was understanding how someone who wants to penetrate a system thinks. He wanted to find "the famous backdoor" in systems and perhaps help close it. To reach his professional goal, he trained himself a couple of hours per day, trying to find security flaws in his own IT equipment.

Some participants aspired to become a pentester because of the variety it offers, because it is not that "you go to work in the morning and you do repetitive tasks

[37] According to the UK National Cyber Security Centre, pen testing is "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might" (National Cyber Security Centre, 2017).

and then you go back home, there is some [thinking] behind it." This is in line with the explanation given by another student, whose predilection for penetration testing stemmed from the approach to this type of security operations. He posited that every software has its characteristics, so discovering software vulnerabilities "is always a challenge, it is never the same." He would like his job to be always stimulating and dynamic, and penetration testing would allow facing challenges he has never encountered before.

6.2.3 "It is like the medical school of computer science": issues in cyber security educational and professional careers

To understand the (perceived or objective) issues at the intersection between cyber security supply and demand, I asked students what obstacles they foresaw in becoming cyber security professionals. It is plausible to think that, if students believed there were insurmountable hurdles on the path to become a cyber security expert, their interest in the topic and a career might weaken over time. Generally, students interested in pursuing a career in the field were confident that, with the appropriate time and resources, they would be able to obtain a cyber security job. However, other students pointed out important issues related to both the supply and the demand side of the labour market, which they experienced first-hand. These limitations pertained to difficulties finding and accessing cyber security-related educational and professional opportunities. Their answers were helpful to expanding the discussion on the cyber security skills shortage and the suitable approaches to mitigate it (ch. 9).

A first obstacle that some students reported was the apparent lack of cyber security courses and degrees. For instance, one student said she would love to pursue a cyber security master's degree but felt they were very selective, claiming that while so many people want to enrol, the educational offering is still limited. She believed that cyber security in general is a "very restricted field" and that:

> "[this] part of the university is very closed: it is like the medical school of computer science."[38]

She argued that very few people are admitted because there are "very high-level professors" and high tuition fees. Moreover, one would need a GPA of 26/30 to be selected, which she considered very high for a computer science degree. She was uncertain about why access is so tough and wondered whether the field is so complex that entering is allowed only to gifted students. She also stated that some of her friends would be interested in enrolling but:

> "almost everyone gives up. They say that if it is so difficult to get in, maybe I am not skilled…it is not the right direction. And therefore people opt for different master's degrees."

I asked her whether all cyber security master's degrees in Italy are so selective, and she answered that not all of them, but on average, this is the case. She gave the example of a cyber security master's degree in Milan, which she thought was one of the best. However, because of the high-level entry requirements, she doubted she would be offered a place if she applied. Another issue was the lack of cyber security courses in her computer science bachelor's degree. She would "definitely" enrol in a cyber security course, but she could not find one at her university, even among the electives.

Another student echoed the same frustration about the presence of face-to-face cyber security courses. He said that he had been trying to look for them, but "they do not exist, in the whole Rome, they do not exist." A reason he gave for the absence of courses was that no one talks about cyber security, and even in his high school for example, the CCIT had not been publicized. He argued that "everyone knows it (cyber security) exists, but no one wants to see it, and therefore they (cyber security professionals) stay under a blanket." He added that, before the CCIT, he had never seen a cyber security expert until the CCIT admission test, where the professor administering the test was an expert:

[38] Admission to medical school in Italy is usually considered tough. For reference, in 2019 individuals admitted to medical school were 12.701 out of 60.776 who attempted the test, thus a 21% acceptance rate (Savino, 2020).

> “Until that moment, they were like unicorns to me...I had never seen one.”

Similarly, another student claimed that cyber security does not encourage one to commit because it is a very “obscure topic.” It is a bit of a “taboo,” and sometimes, it is even hard to find material. Moreover, he claimed it is always associated with something negative: “the impression is that you can always achieve more if you go to the dark side.”

A student’s difficult experience in obtaining an entry-level cyber security job opportunity revealed the current problems affecting cyber security demand in the labour market.

The interviewee had been looking for internships during the summer but stated that it had been challenging to find open positions in cyber security, especially internships and positions with little or no professional experience. This problem was not only confined to the Italian labour market as he had applied for internships anywhere in the world. His summer job search had taught him that:

> “it is not easy for a graduate student to enter cyber security because the sector wants people with experience.”

While this was discouraging, he was not so bleak in his overall assessment of the cyber security labour market. He stated that the lack of experience might mean that the “door is closed now,” but if one has passion and continues to nurture it, that door can be opened again later. His solution was to build his own cyber security portfolio by undertaking personal small cyber security projects to show human resource managers his competences and abilities. Without showing previous expertise, otherwise, he believed it would be challenging to directly enter a company as a junior cyber security professional.

6.3 Summary of findings

Chapter 6 had the goal of assessing the level of participants' cyber security interest before the start of the CCIT. Establishing their baseline cyber security interest was undertaken to gauge the extent to which the CCIT influenced it, which is done in the next chapter. Data were gathered on interest in cyber security as a topic and as a career choice.

Results in section 6.1 demonstrated that interest in cyber security as a topic was high among participants before the CCIT began. Study participants showed their interest through various examples that included routine security operations, enrolment in cyber security courses, participation in skills competitions and reading of specialized material. However, not all those who signed up to the CCIT were drawn to cyber security, which is an unexpected finding given that they voluntarily decided to participate in the competition. These students were not so passionate about cyber security mainly because they were only interested in the programming side of the competition or because they were more interested in other topics, a finding with important implications for this research and which will clearly emerge in chapter 7.

Results in section 6.2 confirmed that interest in cyber security as a career option was also high, and the penetration tester was the cyber security role that students aspired to the most. However, survey results showed that respondents seemed to be more interested in cyber security as a topic rather than as a career choice. This is an important finding that shows how skills competitions' participants might not see interest in a topic and in a career as fully intertwined, which means that a skills competition could influence one outcome variable but not necessarily both. Moreover, in line with findings on cyber security interest as a topic, a minority of students were unwilling to consider a cyber security career because they found other career trajectories more compelling or limited awareness of the cyber security sector.

Students also highlighted some constraints on their path to become cyber security professionals, which are important to consider to understand better the issues affecting cyber security supply and demand. One obstacle that students reported was the limited availability of cyber security courses and degrees, which is one element that could prompt the formation of cyber security interest, as found in section 5.2. Another issue was the lack of entry-level cyber security opportunities, with students reporting companies looking mainly for professionals with prior experience.

7. CCIT influence on cyber security interest and other variables

Chapter 7 aims to understand the extent to which the CCIT influenced cyber security interest, educational and career planning, key education and career choices, and competing interests. Together with chapter 6, it answers the first part of the second main research question: Do NCSSCs influence participants' interest in cyber security as a topic and as a career?

While the next chapter will focus on the “how,” this chapter seeks to answer the question “to what extent?” This chapter is central to the whole thesis. Knowing whether a national cyber security skills competition (NCSSC) influences students’ mindsets and decisions is essential for a complete discussion on the benefits and disadvantages of implementing such an intervention as a skills shortage mitigation policy.

This chapter comprises six sections:

- section 7.1 describes the influence of the CCIT on interest in cyber security as a topic;
- section 7.2 explains the influence of the programme on cyber security as a career;
- section 7.3 reveals how students’ educational and career planning has been influenced by the CCIT;
- section 7.4 discloses if and how CCIT participants altered their key educational and career choices because of the CCIT;
- section 7.5 reports on whether the programme changed their interest in other topics and careers;
- section 7.6 provides a final summary.

7.1 CCIT influence on interest in cyber security as a topic

This section presents survey and interview data on the extent to which CCIT participants' interest in cyber security as a topic changed during the CCIT training programme. It also highlights the factors contributing to this change, although those related to the CCIT will be elaborated upon in the next chapter.

Data suggest that the CCIT had a role in increasing interest among participants, including CG students, whose CCIT experience was limited to the admission process. However, and perhaps not surprisingly, interviews clarified that other elements contributed to the variation of interest in cyber security among CG participants.

7.1.1 Survey results

The second survey (N=390) asked participants whether the CCIT had a direct influence on their interest through the question "Did the CCIT influence your interest in cyber security as a topic?" and produced the following results (figure 24):

- Most participants (71%) stated that the CCIT had either significantly increased (29%) or had increased (42%) their cyber security interest;
- The CCIT had neither increased nor decreased the interest of 27% of respondents;
- Finally, 2% declared that the CCIT had decreased or significantly decreased their interest.

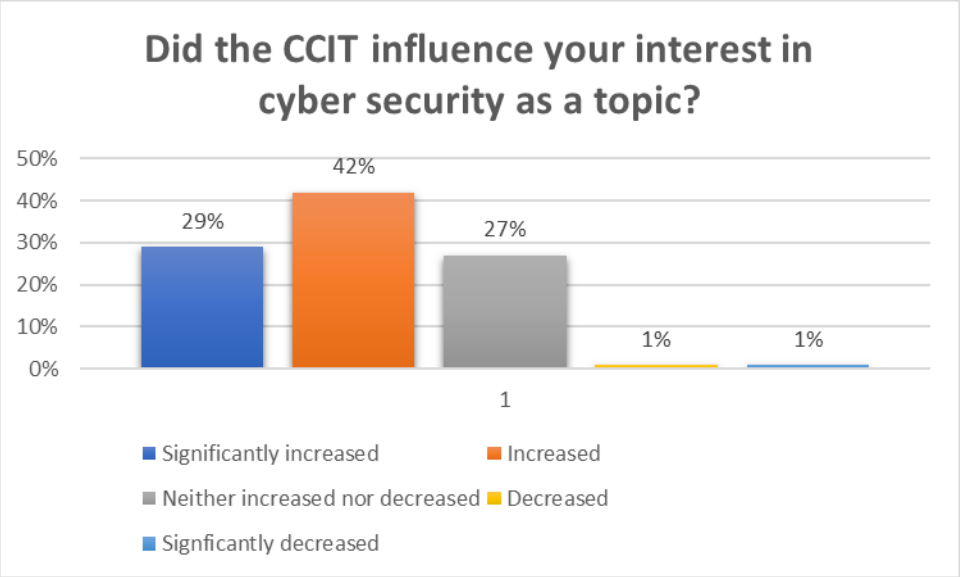

FIGURE 24

In this context, the influence of the CCIT can be better understood when CG and TG responses are compared and, in this regard, one can notice some differences between the two groups (figure 25):

- 78% of TG participants responded that the CCIT had either strongly increased (40%) or at least increased (38%) their interest in cyber security as a topic, compared to 67% of CG participants;
- A higher percentage of CG participants (31% vs 17%) answered that the CCIT had neither increased nor decreased interest in cyber security as a topic;
- Slightly more TG participants (4% vs 2%) had either decreased or significantly decreased their interest in cyber security as a topic compared to CG students.

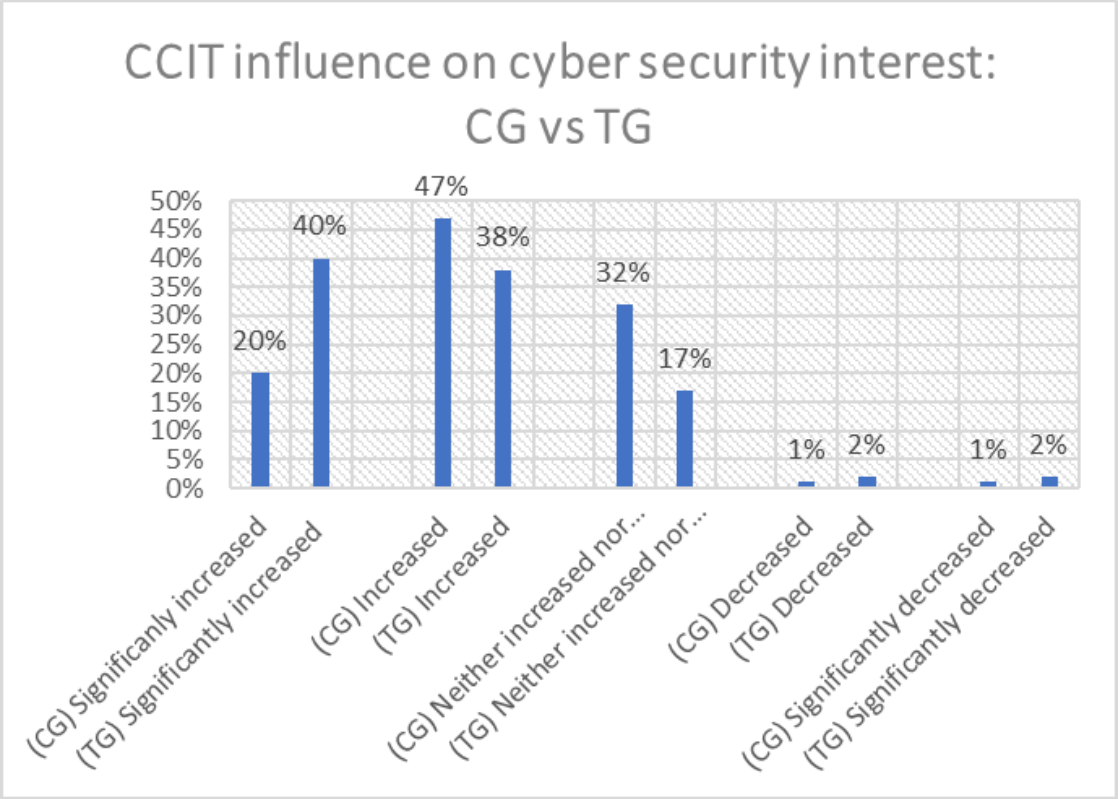

FIGURE 25

7.1.2 Interview results

Interviews with CG and TG participants complemented the results of the second survey. Interviews involved one question when participants were asked to quantify how their interest in cyber security as a topic had changed from February to October 2020 and to justify their answer. Tables 15 and 16 report how study participants quantified variation in their interest in cyber security as a topic. These tables do not attempt to give any statistical representation but rather to offer a numerical overview of their accounts before delving into the qualitative explanation.

In the CG, most study participants (75%, 12/16) reported an increase in their interest in cyber security as a topic, while 25% (4/16) reported no variation (table 15).

TABLE 15

Variation in cyber security interest as a topic in the CG			
Participant	**Before score (2nd interview)**	**After score (2nd interview)**	**Difference**
Avan03	6,5	8	+1,5
Boel22	7,5	8,5	+1
Caed14	8	10	+2
Caid06	6	6	0
Cuem16	8	10	+2
Mami07	8,75	8,75	0
Molo31	6	7,75	+1,75
Most17	8	9	+1
Pahe07	7	9	+2
Pede20	7	8	+1
Pido06	7,75	9,75	+2
Pola07	8	8	0
Ropa25	6	7	+1
Rost0	8	8	0
Stma02	7,5	8	+0,5
Trma18	10	10	0
	7,5 (avg.)	**8,48 (avg.)**	**+ 0,98 (avg.)**

In the TG, most study participants (69%, 9/13) said that their interest had increased, while for 31% of them (4/13), it had either remained constant or decreased.

TABLE 16

Variation in cyber security interest as a topic in the TG			
Participant	**Before (2nd survey)**	**After (2nd survey)**	**Difference (2nd survey)**
Anri23	7	5	-2
Cani30	8	6	-2
Cesi28	8	9	+1
Czro19	8	9,5	+1,5
Gama26	4	4	0
Gari24	8	10	+2
Moma11	4	10	+6
Mona29	9	9	0
Pano15	5	9	+4
Pgro17	8	10	+2
Udel09	5	6,5	+1,5
Vegi07	7	9	+2
Vida12	7,75	9,75	+2
Total	**6,82 (avg.)**	**8,21 (avg.)**	**+ 1,38 (avg.)**

7.1.2.1 Interview results: influence on CG participants

Interviews were helpful in gauging the context and the factors that influenced CG participants' cyber security interest in the period between March and October 2020, when their TG colleagues undertook the CCIT training. Many factors generally contributed to increasing interest in cyber security as a topic among CG students. Perhaps, the most insightful finding was that the CCIT also contributed to this increase, even though CG participants had their experience limited to the

admission test. Perhaps less surprisingly, in some cases, the CCIT had little or nothing to do with increasing their interest.

Many study participants identified the CCIT as a co-factor that made them more attracted to cyber security. Hence, one could argue that the CCIT was associated with their increased interest.

For example, the case of one participant was fascinating in showing how the CCIT, coupled with environmental conditions due to the pandemic, made him realize he had made several mistakes in his life and career choices, which he had been determined to redress since then. He revealed that the lockdown (due to Covid-19) had opened his eyes and had made him comprehend that he had been on the wrong path. If he wanted to achieve something in the cyber security sector, he needed to pursue it fully. The CCIT had an essential role in this process, particularly failing the admission test. He recalled that the admission had left him with a "burning sensation," especially after realising that he would have probably passed the test if he had tackled the tests with the same skills he had developed after February 2020.

At least a couple of students attributed their increased interest to the OCCIT.[39] For example, a student said that the CCIT had had no impact on him because he had not passed the admission test. However, the OCCIT had been a great opportunity, which allowed him to grow. His interest had increased due to the educational material provided, which had made him feel part of the CCIT. Similarly, another student said that the OCCIT had been the cause of his renewed interest in cyber security as a topic, which had led him to get deeper into the subject and understand how cyber security was much more enjoyable than he thought. He argued that previously cyber security had been an "obscure world," and, thanks to the

[39] See section 4.2 for a description of the OCCIT programme. As a reference, according to data communicated by organizers in a private email exchange, out of an eligible population of 1309, 511 students enrolled in the OCCIT programme and 28 received a certificate of attendance. The post-survey received 125 replies (out of 390) from participants who enrolled in the OCCIT: 75% (N=94) joined in without completing it, while 25% (N=31) obtained the certificate of attendance. There was a discrepancy in the data communicated by the organizers about the numbers of individuals who received the certificate of attendance (N=28) versus the number of respondents who *self-reported* to have received the certificate in the second survey (N=31).

programme, he had started looking into what cyber security skills competitions were, how cyber security worked, and the careers of people specializing in this sector.

Not surprisingly, however, other students did not feel the CCIT had contributed necessarily to their augmented interest, but other factors had. The cases of two students are particularly illustrative.

A student said that her interest in cyber security had increased because her university had recently opened admissions to a new master's degree in cyber security and artificial intelligence. In the first February interview, she was doubtful about cyber security because of the difficulty in accessing a related master's degree (due to the high entry requirements). However, the opening of this new master's degree had changed her perspective, and she sounded genuinely excited about this new prospect. Earlier, she felt that accessing a cyber security master's degree would have been almost like a dream: "It was like 2 meters away from me, while now it is like it is 10 centimetres apart, I can see it… (…) it is there, and I can grab it if I want to."

Another student's case was particularly illuminating in explaining how even news coverage could have a bearing on interest, which is in line with what was found in section 6.2.1. He explained that "in this period, there have been numerous cases of data breaches at the global level that make you understand how important cyber security is and how a simple mistake can invalidate your privacy." He corroborated that he had been particularly struck by the Twitter hack case when several famous public figures had their login credentials stolen:

> "At that moment, I realize that if even them, who are considered the untouchables, the non-plus-ultra, could be touched, [one could only imagine what could happen to] us, the populace."

This episode prompted him to become more aware of his personal security, including upgrading the defences of his existing accounts or deleting those he had stopped using by leveraging the provisions of the General Data Protection Regulation with internet service providers.

These findings are related to those in section 8.2.2, showing how CG students positively reacted to the failed admission, which they considered normal in their skills development process. Results in this section add to those findings, showing that not only did this admission debacle not mean CG students became less inclined towards cyber security, but the CCIT contributed to positively influencing their interest, even though it might have not always been the only or primary reason. This is one of the key findings of this study as it counters one of the initial hypotheses stating that the CCIT, more specifically the failure to pass the admission test, would have negatively influenced the cyber security interest of non-admitted participants.

7.1.2.2 Interview results: influence on TG participants

Almost 70% of interviewees declared that their interest in cyber security as a topic had increased between March and October 2020, which they attributed mainly to the CCIT and the training programme. In particular, students valued the enhanced knowledge and skills they received from the training. However, 30% of interviewees had their interest kept constant or reduced.

One of the main reasons the CCIT increased interest in cyber security as a topic in the TG was the training, which enhanced participants' cyber security knowledge and improved their awareness of the sector. For example, one student said that, during the training, professors had explained several topics that he would have never known about or understood by himself. Likewise, another student noted that the CCIT had contributed to his increased interest as earlier he did not know what cyber security was about. He said that even for someone knowledgeable about IT, it is not always easy to understand what cyber security implies, how it is applied and what tasks one performs. However, the CCIT had given him a deeper understanding.

Another student maintained that the CCIT had made him aware that he could achieve anything if he put enough effort into studying and practising. It was the CCIT that gave him this confidence, especially the tutors, who were the students who had undertaken the CCIT's training the previous year. He had been particularly impressed by former students' performances in other cyber security skills competitions, which convinced him that, by studying hard, he could find security vulnerabilities on his own and help companies fix them.

A student underlined the importance of the training but also the timing of the competition. He explained that the CCIT had come when he was feeling lost in his mathematics career and wanted to change his life's objectives. The CCIT was able to instil curiosity in him, which was a determining factor for someone like himself who embraced new experiences also based on their ability to tease him. In addition to coming at the right time, the CCIT had such a profound impact because of the people who managed the training and because of its delivery, which had constantly challenged his new knowledge and skills. In sum, he concluded that:

> "Clearly, the people I met and how the training was delivered was key, meaning that if my first approach to cyber security (i.e. through the CCIT) had been different, namely with poor training or with instructors less interested in helping the participants…probably I would not have decided to continue on this [cyber security] path. Well, then, yes, from this perspective [the CCIT] was key."

Another finding was that, for some participants, interest in cyber security as a topic increased because of their improved awareness surrounding the sector and the profession. This was unusual as one would expect these reasons to explain increased interest in cyber security as a career rather than as a topic.

One participant said that the CCIT had made him notice how "widespread" cyber security is, particularly how being a cyber security professional would make him "essential," which would give him confidence and a sense of security. Moreover, working in the cyber security sector would allow him to apply the tools and knowledge he is passionate about. Although he already knew how important cyber

security is, the CCIT had helped him make this conviction stronger, mainly thanks to lectures and talks delivered by some private companies. Another student acknowledged that his increased interest was due to the CCIT, which had made him discover the cyber security sector more profoundly and had made explicit the possibility of being hired in the field.

However, approximately 30% of TG interviewees either kept constant or decreased their interest during the CCIT programme, citing as explanations the complexity of the cyber security field and previous exposure to cyber security.

For example, one student stated that his interest was lowered from 7 to 5 because he realized that knowing about cyber security requires expertise on multiple levels, which would discourage him in the long run. He made an example of the ISO OSI model protocol stack and explicated that if one wants to create a secure system online, it must start at the code level and then secure all the various components of the system. He admitted that one needs a “wide vision” and much experience, which he is slightly afraid he would not achieve. His case study was fascinating as he is the same student who had been largely dissatisfied with his CCIT experience, reporting various issues with the training programme (see section 8.3.1.5). However, this result is thought-provoking because, during the interview, he did not pinpoint his negative training as an explanation for his reduced interest, but rather what the CCIT made him realize about the field.

By contrast, other participants did not increase their interest because they had already been exposed to cyber security, and the CCIT simply did not add to how they felt about the topic or the sector. For example, a student whose cyber security interest was low even before starting the CCIT confirmed that the programme had not changed how he viewed cyber security. He gave a straightforward explanation:

> “[It did not change my interest] because I was older (than other participants), and I had already been exposed to the topic. So, it was not such a novelty that could drastically influence my perspective.”

This was similar to a fellow TG student, who suggested that he had already known that cyber security was interesting and that the CCIT had not made him change his mind. Certainly, it had increased his knowledge and skills, but not his interest.

These findings should be read in conjunction with those of section 8.3.1, which showed how the two elements that TG students enjoyed the most about their CCIT experience were the training programme and the relationship with the instructors. The results of this section showed that the training was important in students' assessment of the CCIT, and it also contributed to positively influencing their interest in cyber security more generally. This is one of the key findings of this study as it counters one of the initial hypotheses, which stated that the CCIT would have neither increased nor decreased the interest in cyber security as a topic of TG participants.

7.2 CCIT influence on interest in cyber security as a career

This section presents survey and interview data on whether CCIT participants' interest in cyber security as a career changed during the CCIT training programme. It also identifies the factors contributing to this change among study participants, especially CG ones. Factors related to the CCIT will be elaborated upon in the next chapter.

An important result is that the CCIT had a more significant positive influence on interest in cyber security as a topic compared to cyber security career interest. Moreover, data suggest that the CCIT had a more significant influence on TG participants. The CCIT also influenced cyber security career interest among CG students, but not surprisingly, other elements contributed to it.

7.2.1 Survey results

The second survey (N=390) directly asked participants whether the CCIT had influenced their interest in cyber security as a career and produced the following results (figure 26):

- Almost half of participants (49%) confirmed that the CCIT had either significantly increased (13%) or had increased (36%) their interest in a cyber security career;
- 46% responded that the CCIT had neither increased nor had decreased their interest;
- The CCIT had decreased or had significantly decreased their interest in the perspective of a cyber security job for 4% of respondents.

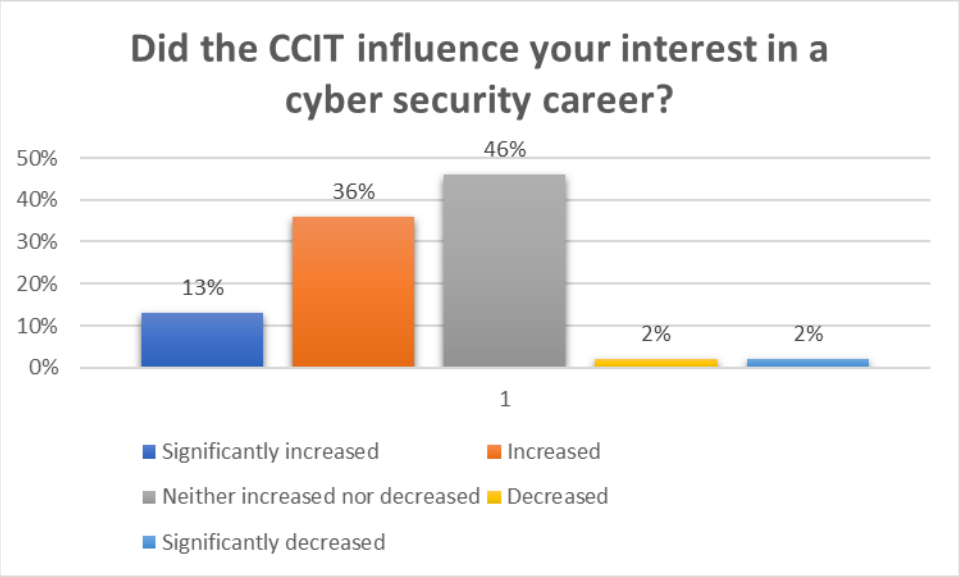

FIGURE 26

An important finding is that the CCIT had a greater influence on participants' interest in cyber security as a topic rather than as a career. In fact, 71% of participants had their interest in cyber security as a topic either increased or

significantly increased due to the CCIT, compared to 49% who stated the same about their cyber security career interest. Moreover, a higher percentage of respondents declared that the CCIT had neither increased nor decreased their interest in cyber security as a career (46%) compared to respondents who gave the same answer but for interest in cyber security as a topic (27%). Finally, slightly more students suggested that the CCIT had decreased or significantly decreased their interest in cyber security as a career (4%) compared to students who declared the same about interest in cyber security as a topic (2%).

This finding has two important implications. First, it confirms that interest in cyber security as a topic and as a career do not always go hand in hand, meaning that CCIT participants might be interested in cyber security as a topic but might be less so in a cyber security career. Second, this result has consequences for the organization and implementation of a national skills competition as it should not be assumed that such an event will be able to positively influence interest in a cyber security career as much as interest in cyber security as a topic. Chapter 9 will analyse this in-depth.

Similarly to what was found in the previous section, the influence of the CCIT on the career interest of TG participants was more conspicuous (figure 27):

- In the TG, 62% of respondents stated that their cyber security career interest had either significantly increased or had increased by the CCIT, compared to 45% in the CG.
- More CG respondents were neutral than participants in the TG (50% vs 33%).
- Slightly more respondents in the CG compared to the TG (6% vs 4%) reported that the CCIT had either decreased or had significantly decreased their professional interest in cyber security.

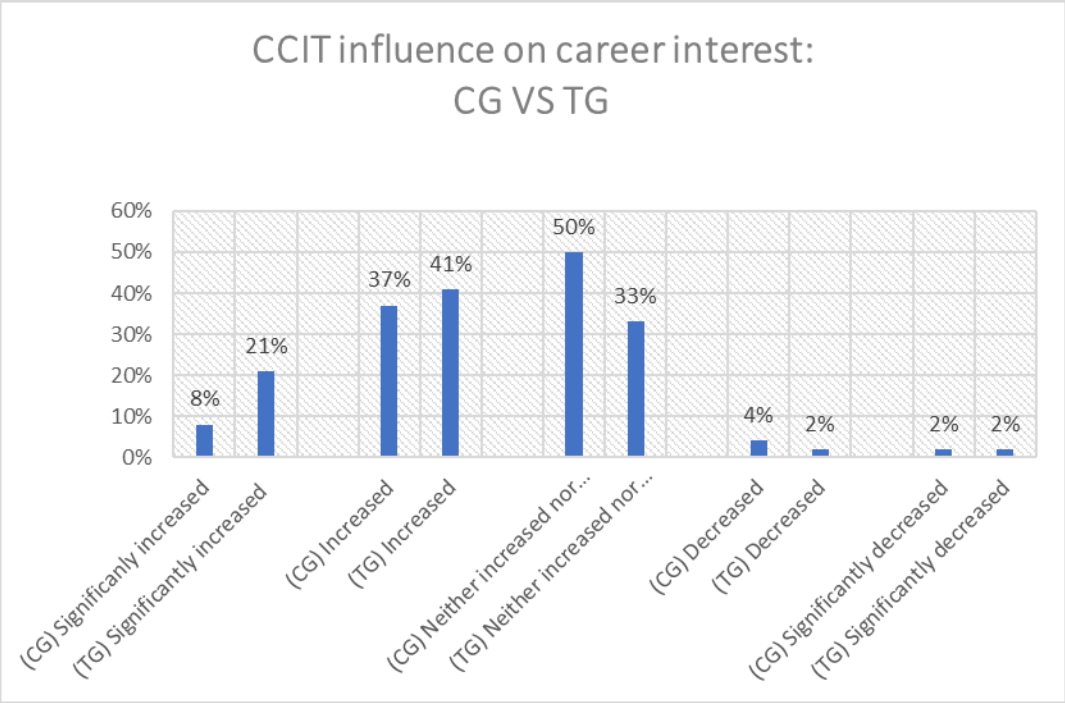

FIGURE 27

7.2.2 Interview results

As for interest in cyber security as a topic, survey results were complemented by interviews. Even in this case, I followed the same protocol, namely I first asked participants to quantify how their interest in cyber security as a topic had changed between March and October 2020 and justify their answer. Results on variation in cyber security career interest are provided in tables 17 and 18. Again, the tables are presented not for any statistical purpose but to provide an overview of how students quantified their variation in cyber security career interest in the CCIT period.

In the CG, 80% of students (12/15) claimed that their cyber security career interest had increased, two students reported no change, and one declared his cyber security interest had considerably dropped (-3) (table 17).

TABLE 17

	Variation in cyber security career interest as a topic in the CG		
Participant	**Before (2nd survey)**	**After (2nd survey)**	**Difference (2nd survey)**
Avan03	6	7,75	+1,75
Boel22	7	8,5	+1,5
Caed14	5	6	+1
Caid06	4	4	0
Cuem16	7	9	+2
Mami07	-	-	-
Molo31	5	7	+2
Most17	7	9	+2
Pahe07	7	8	+1
Pede20	7	8	+1
Pido06	5,75	8,75	+3
Pola07	7	7	0
Ropa25	6	3	-3
Rost20	7	8	+1
Stma02	8	9,5	+1,5
Trma18	8	9	+1
	6,45 (avg.)	**7,5 (avg.)**	**+1,05 (avg.)**

In the TG, 85% of the interviewees (11/13) confirmed that their cyber security career had increased, one student reported no variation, and one student stated his interest had decreased (table 18).

TABLE 18

	Variation in cyber security career interest in the TG		
Participant	**Before (2nd survey)**	**After (2nd survey)**	**Difference (2nd survey)**
Anri23	7	5	-2
Cani30	7	8	+1
Cesi28	7	8	+1
Czro19	7	9	+2
Gama26	3	3	0
Gari24	8	9	+1
Moma11	6	10	+4
Mona29	6	10	+4
Pano15	6	8	+2
Pgro17	8	10	+2
Udel09	5	6,5	+1,5
Vegi07	7	9	+2
Vida12	7	9	+2
	6,46 (avg.)	**8,03 (avg.)**	**+1,58 (avg.)**

7.2.2.1 Interview results: influence on CG

Similar to the results in the previous section, interviews were interesting in explaining changes in students' feelings and perceptions. In the CG, some students reckoned the CCIT experience helped augment their interest in the cyber security profession, but many included other factors such as attending cyber security conferences and news coverage.

One student declared that his increased interest was due to better awareness and the new information he received about cyber security careers. He named two elements that made him more interested in cyber security: the educational material

of the OCCIT and the account of the CCIT training and national challenge provided by his friend who had been admitted to the programme.

Some students attributed their increase in cyber security career interest to their new awareness about the cyber security sector, which they said derived from their CCIT experience. Nonetheless, their explanation about how this happened was not always clear, given that their CCIT experience had been limited to the admission process. In this context, one student advanced that his “new” cyber security knowledge increased his confidence: “the fact that I have this new knowledge, the possibility to say, ok, I can do it as well, I am able to do it as well, it made me grow my interest for a [cyber security] career.”

However, many study participants had their cyber security career interest positively influenced for different reasons. The examples of two students were particularly enlightening. One student went to a cyber security conference, where he realized that there was a great demand for cyber security professionals, and, most importantly, he noticed the lack of competency of some so-called cyber security experts. At the conference, he observed that many who worked in cyber security did not have a “360° knowledge” of cyber security issues. He made an example of the conference chairman, who had made several “coarse” mistakes, which an introductory course in cyber security would have taught you to avoid. At that point, he realized that if this was the general competence level of cyber security professionals, students with an education in cyber security would have good chances to find exciting professional opportunities: “this was the turning point that made my interest grow.”

Another student stated that her cyber security career interest had been rising because news prompted her to do new research on cyber security jobs. One day after her failed admission attempt, she stumbled across some news about cyber security accidents, which made her look more deeply into the kind of professionals dealing with them. During the first interview, she had stated she was interested in cyber security, but it was something generic:

> “I knew about cyber security, but I saw it as a topic, like mathematics…but well, even within mathematics, there are various subjects, like arithmetic, geometry, there are other things. I considered [cyber security] as a single block…however, now I realize there are many, many cyber security roles, which are all different from one another.”

From that realization, she started finding out what potential roles she might be interested in. She admitted that her interest had also changed thanks to discovering these new roles and the possibility of being a professional involved in similar tasks.

However, not all students reported an increase. One student’s interest decreased from 6 to 3, the reason being related to the CCIT admission process. As its case study is useful to describe the original (disproved) hypothesis of this research, the account of his experience is provided in section 8.2.2.

7.2.2.2 Interview results: influence on TG participants

Participants in the TG usually attributed their increase in cyber security interest to the CCIT, namely how the programme showed the example set by the instructors, how demand exceeds supply in the current cyber security labour market and the extent to which the sector is intriguing and potentially lucrative.

For example, one student said that he had been stimulated by his CCIT instructor, a cyber security researcher and professor. He considered his professor’s activity exciting, as his research allowed him to increase his knowledge every day. Considering that cyber security varies a lot, his professor set an example that inspired him to consider cyber security as a job option.

Another student explained that his cyber security career interest had increased because of his new awareness of the sector. Before the CCIT, he did not know exactly what cyber security was, although it was something that “sounded nice.” Instead, with the training, he had developed the knowledge to understand what

this was about, what one could do, and what he could theoretically achieve in his life.

Another student shared a similar opinion, stating that the CCIT had made him understand that “everything is possible.” Moreover, his interest had increased by looking at the labour market demand for cyber security professionals, which exceeded supply. He said that his understanding of the labour market stemmed from reading online blogs and informative sessions at his university.

One of the most enlightening cases was a student who explained that his interest in cyber security as a topic had decreased, but his cyber security career interest had increased, which shed some interesting insights on the complex dynamics of interest development and vocational interest. This student said that his cyber security topic interest had decreased from 8 to 6, even though this decrease had not been due to the CCIT. Actually, the CCIT had the opposite effect, as it allowed him to know more about the sector and contributed to raising his interest. The problem was the current labour market. He argued that it is too difficult for a new graduate with no professional experience to enter the cyber security labour market, making an example of the limited number of cyber security internships. This is a position that the student had also expressed before starting the programme in the first February interview (see section 6.2.3), which apparently the CCIT had not changed. He pointed out that, in the past, he had had interviews involving algorithms and dynamic programming and, therefore, it was not convenient or efficient for him to retrain himself and study further to tackle cyber security interviews. This is why his interest in cyber security as a topic had decreased by two points. On the other hand, though, the CCIT had shown him that the cyber security sector was interesting, with “open challenges,” which is something essential to feed his interest, as well as lucrative stipends. Therefore, his cyber security career interest had increased from 7 to 8 for the possibility of landing a cyber security job in the future. A new career plan backed his hope:

> “I think the topic is interesting, there are many professional opportunities, but being [myself] a new grad, it is easier I will become a software engineer and then become a security engineer.”

7.3 CCIT influence on education and career planning

This research also investigated whether CCIT participants had developed any educational and career plans specific to cyber security. This is one of the themes that emerged from the first round of data collection, which was deemed worth further exploration. The expectation was that students with interest in cyber security would have thought about concrete educational possibilities and professional opportunities to substantiate and further develop their interest in the future.

The main finding is that participants were often unable to articulate a vision, or at least some intentions, related to their future choices. This finding is relevant as it allows us to discuss more broadly the relationship between interest development and vocational interest and the use of interest as an outcome variable in the context of NCSSCs (section 9.4).

7.3.1 Education planning

One of the questions in the second survey (N=390) asked whether CCIT participants were interested in *specific* cyber security degrees. It generated the following results (figure 28):

- Most respondents (45%) did not know of any specific cyber security degree;
- Only 22% replied with a firm yes, while 13% answered that they could be interested;
- 19% responded that they were not interested in any specific cyber security degree.

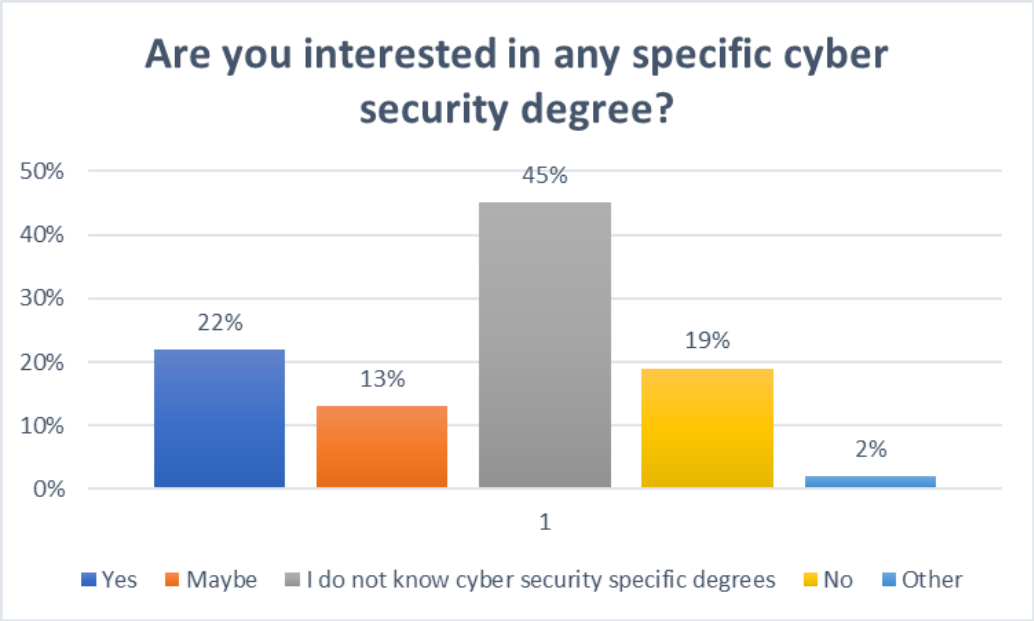

FIGURE 28

The interviews generally reflected these results, with a mix of considerations making students reluctant to think more thoroughly about their educational planning.

For example, one student from the CG clearly showed overall interest in cyber security and a related degree but admitted he did not know any educational path leading to it. He also showed difficulty in articulating what he would subsequently like to do or become:

> "What I am about to tell you is probably not the right term to describe what I would like to do…But, I repeat, I have not had any experience so far…I would like to do something that is related to cyber security, not only regarding emails but also basic information systems…Maybe not even for companies, but maybe for the common user. I am not sure whether a term to describe what I am saying exists."

When asked whether he was interested in obtaining a cyber security degree, another student epitomized the question as "tough," adding he did not have a clear idea. He had looked into some master's degrees offered at his home university and the University of Bologna, but he had not decided what to do yet.

Similarly, a student said he wished to receive further cyber security training but did not know many cyber security degrees. He was in his last year of high school and planned to enrol at his hometown's university, which is 7 km away from his home and therefore represented a natural and financially sustainable solution.

7.3.2 Career planning

Even more evident results were related to knowledge of *specific* cyber security jobs (figure 29):

- 55% did not know any particular job role within cyber security;
- 17% of participants stated to be interested in a specific cyber security job role, and 11% could be interested;
- 17% were not interested in any precise role.

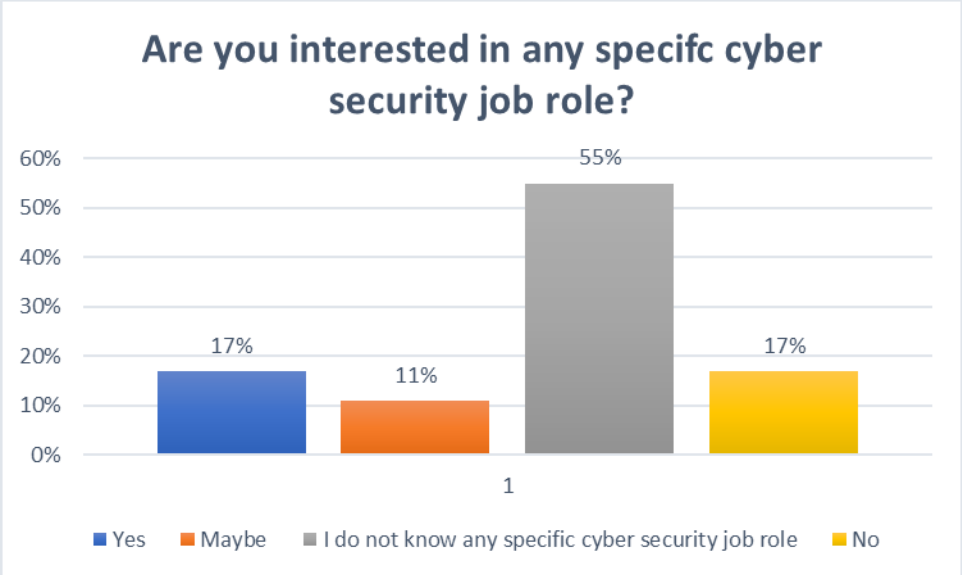

FIGURE 29

Interviews showed even more vehemently that students had not yet thoroughly thought about potential careers, with participants often assuming a "wait and see"

approach given the lack of knowledge regarding the sector. For example, a participant was interested in a cyber security job but declared:

> "I do not know any of them, so I can't tell. (…) I have no idea how a cyber security job in a company looks like."

He knew some activities that a cyber security professional could perform, for example, analysing a malware bytecode and then performing a forensic analysis. However, generally speaking, he did not believe himself to be well informed about job opportunities in cyber security. When I asked him whether he was interested in a professional certification, he admitted, "No, unfortunately, I do not know what they are…I discovered them now, good to know."

A student claimed to be very interested in a cyber security degree and to want to become a cyber security professional one day. Nonetheless, he did not know what a cyber security professional could do, although he was aware that "various tests can be performed to understand whether a malicious person can enter a system or not." He had given his cyber security career interest a score of 9, but he added that he was also very interested in the salary. Hence, even if the job was satisfying, he would not be entirely pleased unless paid well.

A couple of students demonstrated well with their quotes how far away they thought the right time to start thinking about a career was. One student revealed that he had never considered a particular security job role because:

> "I do not really know what the future holds…I do not know where my studies will lead me or what field will arouse me more. I cannot say at the moment."

Instead, another student had already considered a career in the sector ("it is a nice idea") but revealed he had put little thought into it:

> "maybe a company…yes, I would like that, but who knows, time will tell."

7.3.3 Difference between CG and TG

When comparing CG and TG results, TG participants seemed to be slightly more aware of the types of cyber security degrees available, which might indicate that the CCIT had a more significant influence on TG participants in clarifying the potential educational paths to follow (figure 30):

- 25% of TG participants, as opposed to 20% in the CG, said they were interested in a specific cyber security degree;
- Likewise, 33% of TG students stated they did not know about specific cyber security degrees vis-à-vis 48% in the CG;
- Interestingly, however, this increased awareness of cyber security degrees was also reflected in the answer "I am not interested in any specific cyber security degree," which 15% of individuals in the CG and 26% in the TG claimed.

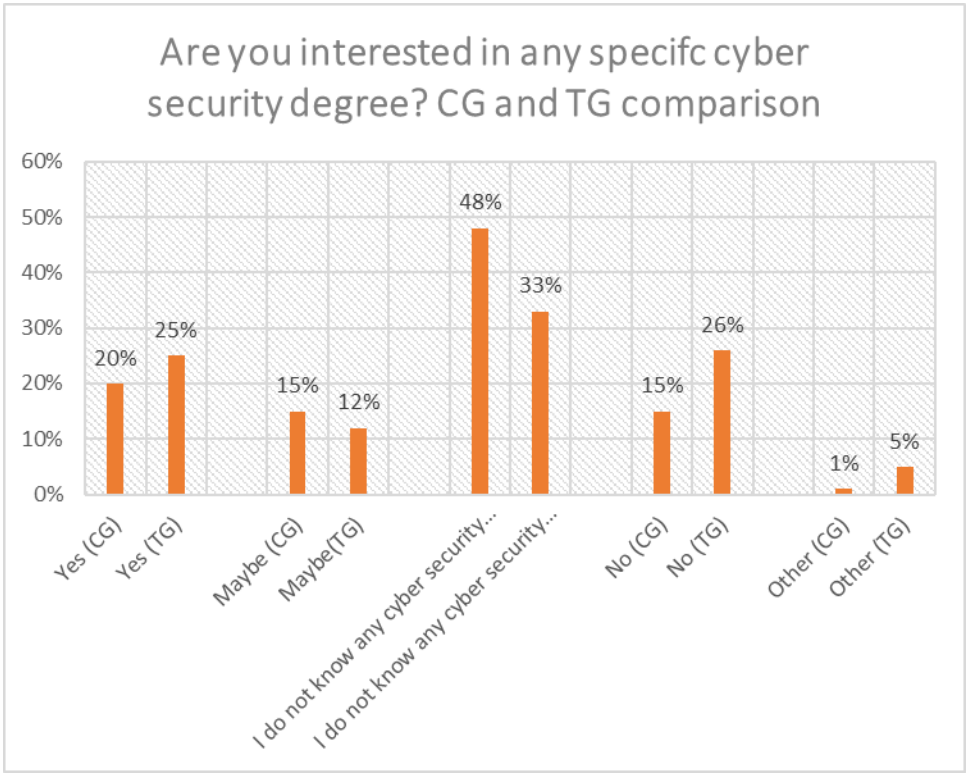

FIGURE 30

The interviews confirmed the trends emerging from the survey, with TG students usually showing moderately more explicit ideas on how to continue their education in cyber security after the CCIT programme. In fact, while CG students usually had more generic plans concerning enrolling in computer science degrees and then perhaps following some cyber security courses, TG students could usually pinpoint cyber security degrees in specific universities. Overall, their educational planning appeared more advanced.

Similar results emerged when the survey asked whether CCIT participants would be interested in a specific cyber security job (figure 31). Even in this case, individuals from the TG appeared to be more inclined towards specific cyber security jobs than CG students:

- 33% of TG students declared to be either interested or potentially interested in exact cyber security roles, compared to 23% in the CG;
- Perhaps more illuminating, 59% of CG students admitted they did not know any specific job role within cyber security, as opposed to 44% in the TG;
- Similarly to what happened with degrees above, however, the TG group seemed slightly more decisive in ruling out any specific job role interest within cyber security (21%) than the CG (18%).

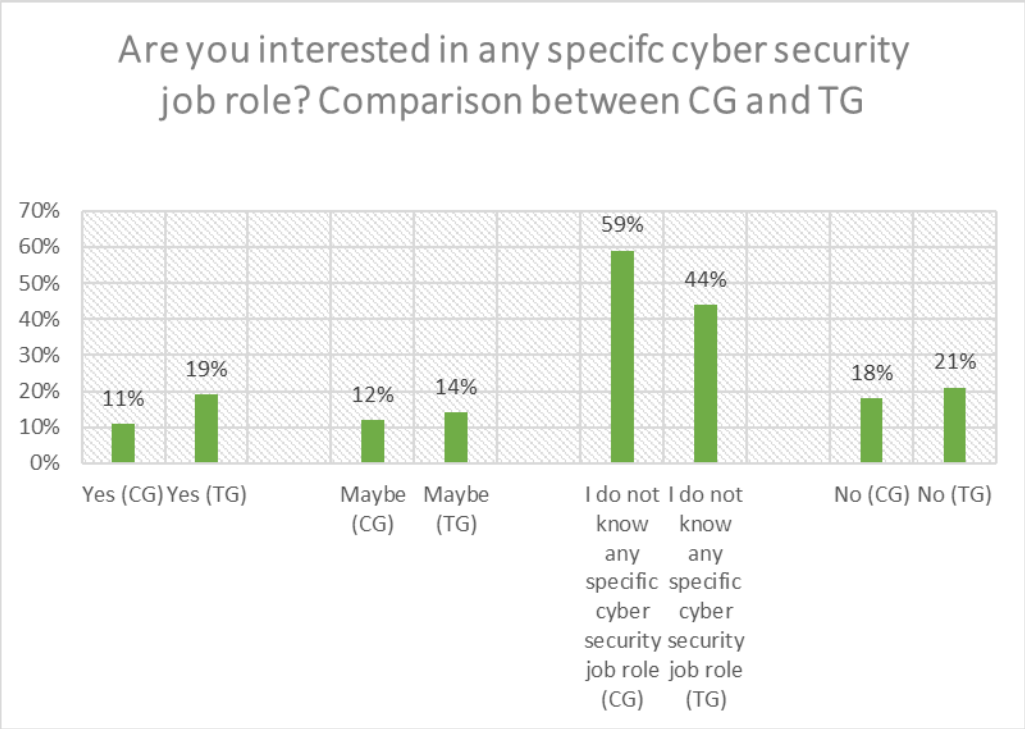

FIGURE 31

Interviews data reiterated these findings, with CG students showing a lower level of awareness regarding the cyber security sector or the job opportunities it could offer. For example, a student in the CG said that they were generally interested in a cyber security job, but nothing more specific as he had no clear ideas about potential cyber security roles. Whereas he knew that in programming various roles are assigned according to competencies, he did not know how this would work in cyber security.

On the other hand, TG students seemed slightly more informed, often mentioning the penetration tester as their preferred path into cyber security (see section 6.2.2).

7.4 CCIT influence on educational and career choices

As stated in section 4.2, the Covid-19 health emergency delayed the second round of data collection by three months. Nevertheless, this unwanted delay had the

positive consequence of finding out whether the CCIT influenced participants' key educational and professional choices in some manner. This was possible because, initially, the second data collection should have occurred in July 2020, when many students would not have taken decisions about their future steps yet. Instead, the second data collection took place between October and December 2020, when the new academic year had already started and when students had already made key educational choices or had entered the professional world.

Investigating the extent to which the CCIT influenced participants in these key decisions is vital as it provides further clues on the value of the concept of interest when framing and assessing NCSSCs (section 9.4). Even though only a limited portion of CCIT participants took these key decisions, results imply that the CCIT had some influence on key educational choices of its participants, especially TG students. Unfortunately, data on professional choices were too limited to draw any conclusion. Because of insufficient information stemming from interviews, this section will only present data collected through the second survey (N=390).

7.4.1 Survey results

In the second survey (N=390), 28% of CCIT participants (110/390) stated they had changed their "status" (figure 32):

- 14% had either enrolled in a bachelor's degree;
- 11% had enrolled in a master's degree;
- 4% had started working/looking for a job;

The CCIT either influenced or partially influenced the decisions of 49% (54/110) of these students.

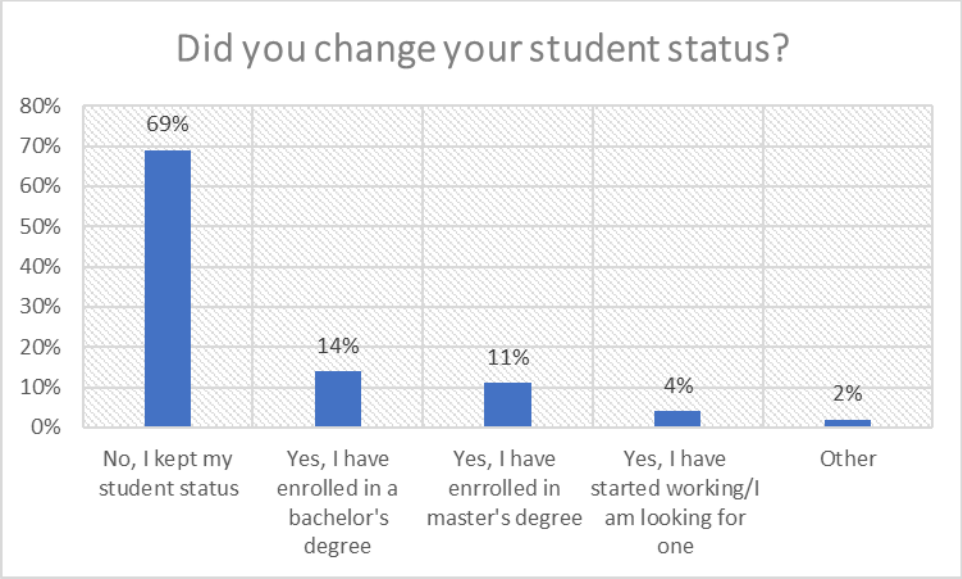

FIGURE 32

Of the 14% of students who graduated from high school and enrolled in a bachelor's degree (figure 33):

- 60% enrolled in a computer science or computer science-engineering degree and had intentions to follow cyber security courses;
- 13% enrolled in such degrees but had no aspiration to follow any specialized cyber security course;
- 13% did not enrol in such a degree;
- The CCIT either influenced or partially influenced the choice of 57% (N=26) of them. The influence of the CCIT on these 26 participants was likely "positive," as 81% of them enrolled in a computer science degree and had the intention to enrol in cyber security courses. Moreover, 89% stated the CCIT had either significantly increased or increased their interest in cyber security as a topic; 77% had their cyber security career interest either significantly increased or increased.

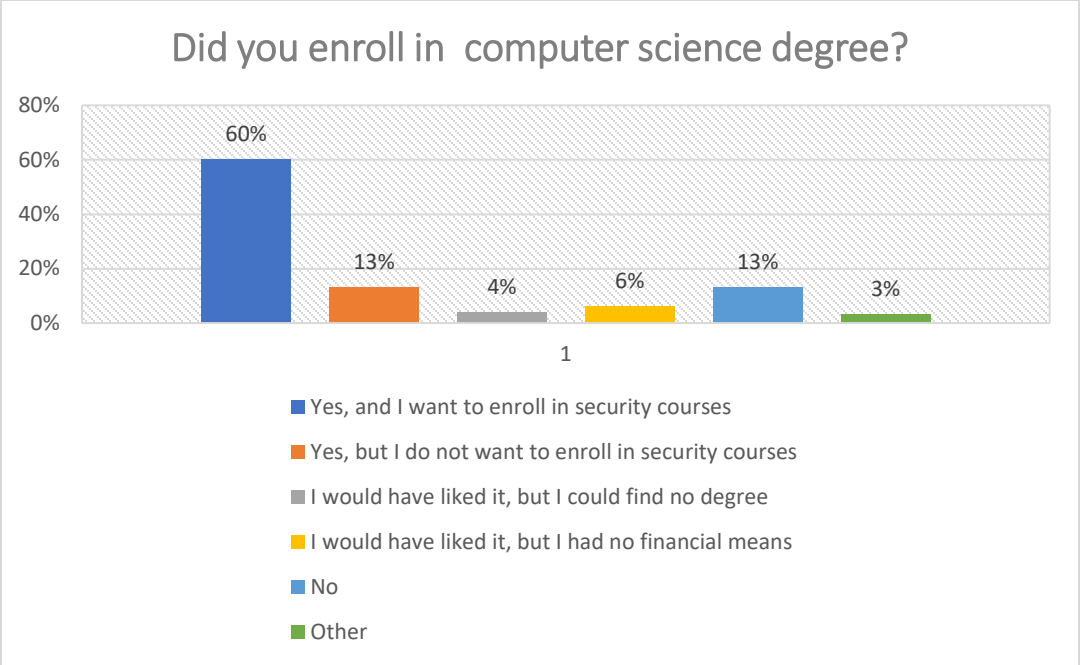

FIGURE 33

If one compares CG and TG results (figure 34), some interesting differences emerge:

- 78% of TG participants enrolled in a computer science degree and wanted to pursue cyber security courses, compared to 57% of participants in the CG;
- 22% of TG participants had enrolled in such degrees but did not want to follow a class in cyber security compared to 17% in the CG;
- 78% of TG participants were either influenced or partially influenced by the CCIT when making their choice, compared to 48% in the CG.

An open-ended question asked respondents to clarify how the CCIT had influenced their decision and, while no one from the CG replied, some students from the TG reiterated that the CCIT had a “positive” influence, as it:

- Laid the foundation for future studies;
- Made understand what a cyber security expert does;

- Encouraged to get deeper into the subject;
- Confirmed their passion for the topic;
- Made understand that it is essential to protect personal projects.

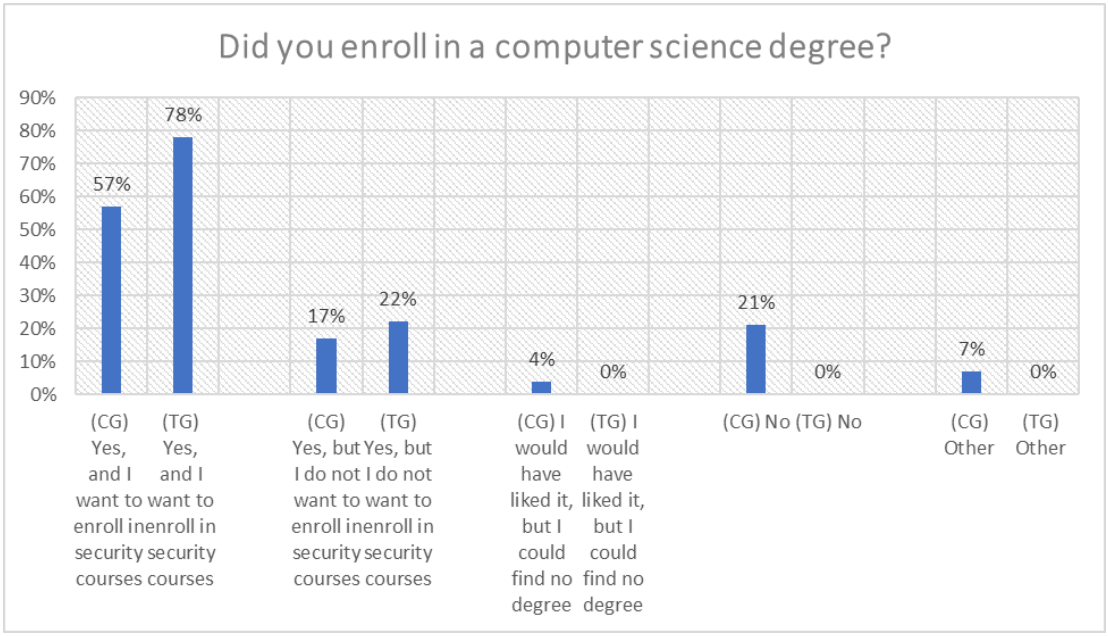

FIGURE 34

Of the 11% of participants who graduated and went on pursuing a master's degree (figure 35):

- 39% enrol in a cyber security master's degree or similar;
- 29% did not enrol in a cyber security degree but wanted to attend cyber security courses;
- 32% did not enrol in a cyber security master's degree.
- The CCIT either influenced or partially influenced the choice of 53% (N=21) of them. Again, the influence of the CCIT on these 21 participants was likely "positive" as 48% of them enrolled in a cyber security (or related) master's degree, while 24% did not but had the intention to enrol in cyber security courses. Moreover, 81% of them stated that the CCIT had either

significantly increased or increased their interest in cyber security as a topic, and 62% had their cyber security career interest either significantly increased or increased.

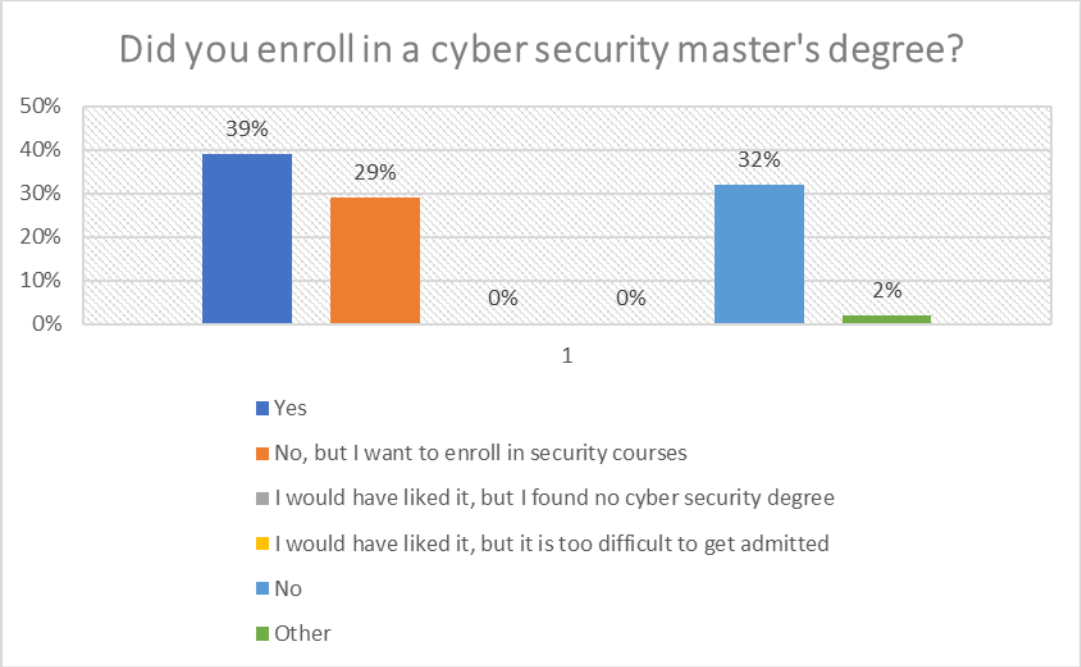

FIGURE 35

When comparing CG with TG students (figure 36):

- 55% of TG participants enrolled in a cyber security master's degree or affiliated degree, compared to 29% of students in the CG;
- 50% of CG students did not enrol in such a degree but wanted to enrol in cyber security courses compared to 9% in the TG;
- 32% of TG participants did not enrol in such a degree, as opposed to 21% in the CG.
- 67% of TG participants were either influenced or partially influenced by the CCIT when making their choice, compared to 46% in the CG.

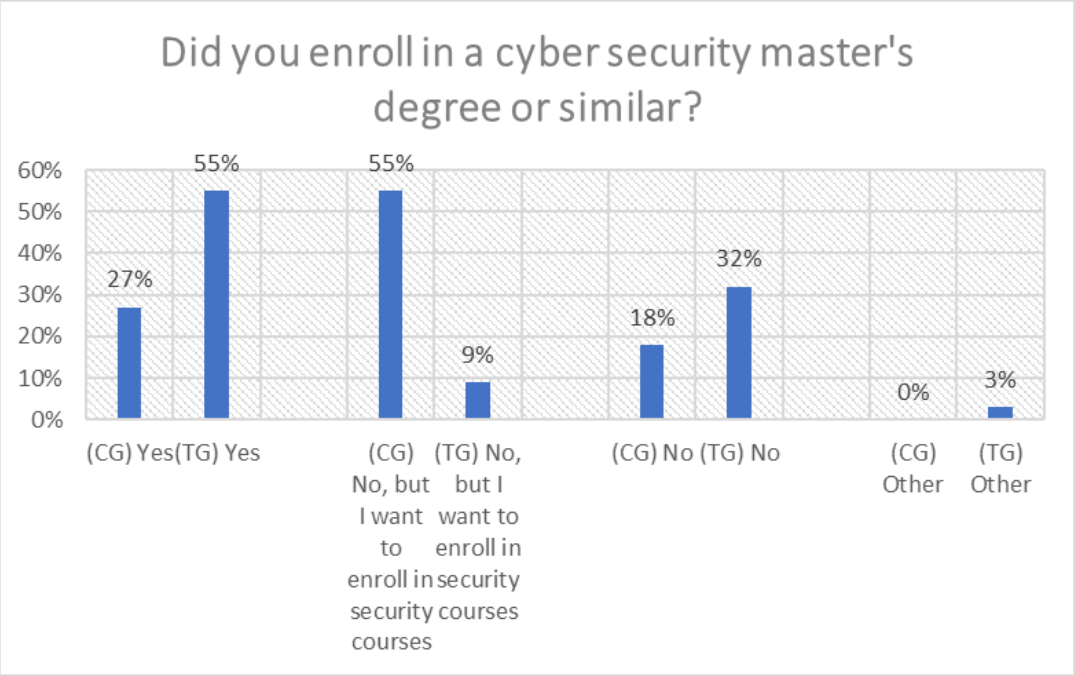

FIGURE 36

Another open-ended question within the survey asked respondents to clarify how the CCIT had influenced their decisions. Some students in both the CG and the TG replied. Interestingly, in the CG, the CCIT had a more “positive” influence, with one student, for example, revealing that after solving some of the cyber security challenges (likely for the OCCIT programme), he had realized how “fantastic” the sector was and he had decided to enrol in a master’s degree with a cyber security curriculum. In the TG, instead, the only two students who replied suggested that the CCIT had had a “negative” influence, making them realize that cyber security was not the right field for them. However, for some, realizing this could be considered a “positive” outcome as the CCIT helped them understand that other educational and career options were more suitable than cyber security.

Finally, the survey asked participants whether anyone had started working or looking for a cyber security job after the CCIT and a small number of students (N=16) answered affirmatively (figure 37):

- 50% started working in cyber security or related areas;
- 19% did not start working in cyber security but wanted to specialize in this field subsequently;
- 19% would have liked the idea of joining the cyber security ranks but found no opportunities;
- 13% did not start working in cyber security or affiliated areas;
- The CCIT either influenced or partially influenced the choice of 44% (N=7) of them. The influence of the CCIT on these seven participants was likely "positive," as 86% either started a cyber security job or wanted to progressively specialize in cyber security. Moreover, 86% of them stated that the CCIT had either significantly increased or increased their interest in cyber security as a topic, and 86% had their cyber security career interest either significantly increased or increased.

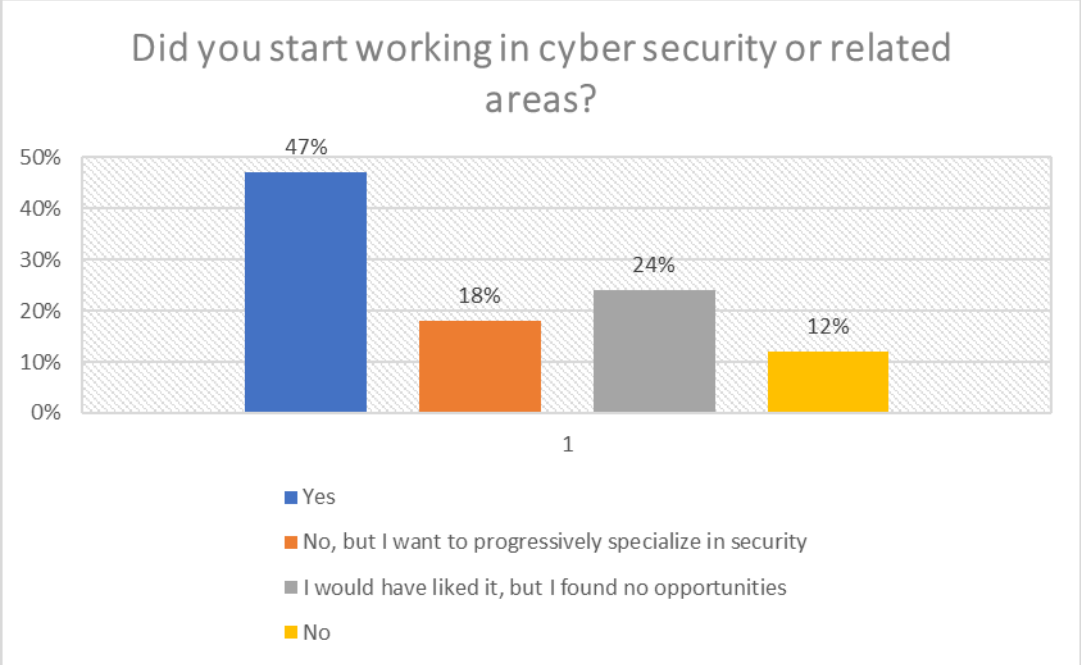

FIGURE 37

In the CG, two students started working in cyber security, and two would have liked to but found no opportunities; the CCIT did not influence the choice of 3 out of 4 students. In the TG, only one student started working; three had the goal to progressively specialize in cyber security; and two did not start working in cyber security. Among them, 4 out of 6 said that the CCIT influenced their decisions.

7.5 Beyond cyber security: topic and career alternatives to cyber security

A key theme that emerged from the first data collection was whether participants attending NCSSCs had other interests in addition to cyber security and to what extent these "competed" with each other. Knowing if this is the case helps to put into context any assessment of the influence of a NCSSC. Change in cyber security interest is an important indicator to understand the effect of an NCSSC, but could be insufficient to appreciate the full context of students' aspirations and intentions. Even when a NCSSC increases students' interest in cyber security, this does not automatically imply that students will permanently lean towards cyber security. Students might enter the competition with interests in other topics and careers, which a NCSSC might not necessarily decrease. The consequence would be that these "competing interests" might still persist and grow despite any influence exerted by the skills programme. This section presents quantitative and qualitative data suggesting that, despite having enrolled in a particular skills competition such as the CCIT and showing high interest in cyber security, very few participants were fully committed to cyber security alone.

7.5.1 Survey results

The second survey (N=390) asked whether participants had any educational or professional "alternatives" to cyber security. A significant result was that only a

minority of CCIT participants seemed to be “completely devoted” to cyber security (figure 38). In fact:

- only 16% of participants responded that they would prefer to stay within the cyber security sector;
- 51% stated that, while they were interested in cyber security, they were interested in other topics and careers at the same level;
- 25% were interested in cyber security but claimed other topics and careers interested them more;
- finally, 8% stated that they wanted to pursue other fields and career paths.

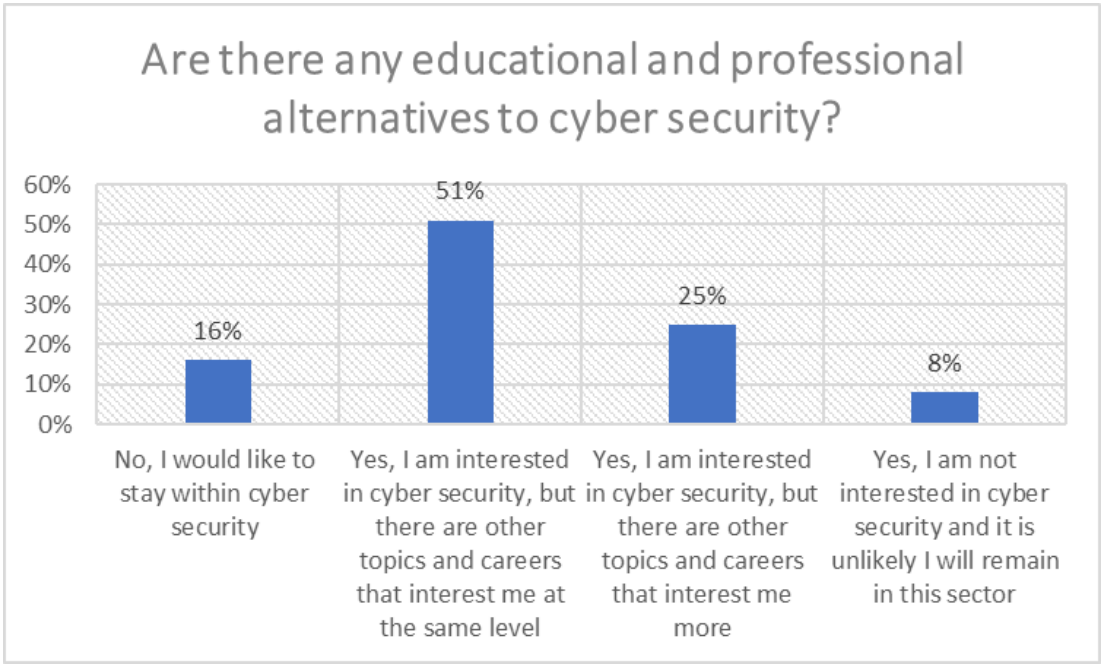

FIGURE 38

Among the various alternatives to cyber security, those most cited were (figure 39):[40]

- artificial intelligence (AI) (55%)
- generic programming (35%)
- software engineering (24%)
- Internet of things (22%)

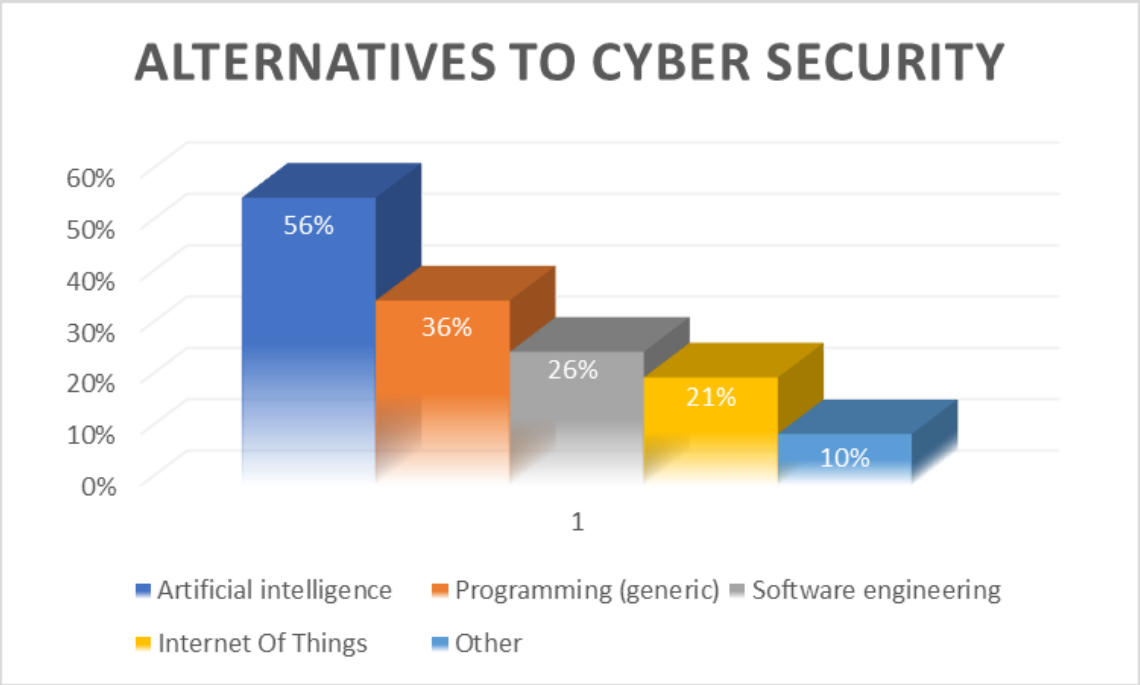

FIGURE 39

7.5.2 Interview results

Interviews were able to dig deeper and elucidate the relationship between interest in cyber security and other topics or career trajectories. They were instrumental in explaining how cyber security interest can coexist with other passions, why and how participants picked alternative interests and the extent to which they might

[40] Respondents had to choose at least one and up to two choices.

prefer them over cyber security. They also confirmed survey results, reiterating that CCIT participants saw AI and programming as the best alternatives to cyber security.

7.5.2.1 Artificial Intelligence

Approximately 40% of participants mentioned AI as an alternative topic and career path to cyber security, which they saw as a fascinating sector given its multiple applications and the advancements it could bring to other fields.

For instance, one student noted that both cyber security and AI were “rising sectors,” so embarking on a career in one of them was a good idea. He started to be interested in AI during his bachelor’s degree, where he had a taste of the topic. He was interested in understanding how some IT tasks could be facilitated using this technology: “So, this is fundamentally my approach, (…) how certain activities that are today considered laborious can be optimized using AI in the future.” He was sure that AI solutions would become instrumental in the development of other technologies, be they in cyber security, medicine or other sectors: “Therefore, my interest is more in what AI brings more than the way it is done.” He argued that these fields go hand in hand and offered examples of some cyber attacks, which could not have been possible without AI tools. Hence, the cyber security expert should have some knowledge of AI and machine learning and be able to link these fields together. He concluded that he would love to study both fields and intended to write about their interrelationships in his university thesis.

Other participants gave even more articulated accounts of their interest in AI, showing how this had been cementing over the years and over other interests, including cyber security.

For instance, one student stated that this passion started from a question he had been asking himself since his childhood, namely how “to obtain the maximum

output with the minimum effort." He explained that his first solution was to create an algorithm able to perform any task, but he soon realized that optimizing it would have been too complicated. Then, while searching online, he came across AI:

> "And I said to myself, this is what I need…because it can substitute humans in any task. I am very fascinated by the development of AI."

He has continued to feed this interest by watching videos online and looking for information, and he would love to develop his AI interest because "this is the biggest (interest) I have."

Another student explained that he became particularly inspired by AI after watching online videos showing how a computer can detect faces and connect dots in a way a human cannot. Following this, he undertook a couple of projects using the TensorFlow library and continued to consult material online. He had no specific educational plan for now, and, while developing one, he was copying other people's projects to understand how they approached them. He posited that cyber security has a very steep learning curve, and he believed a newcomer could not start doing expert tasks right away. Even AI is hard, but he judged the learning curve to be less steep: "If you know how to create a neural network, you will have a job."

7.5.2.2 Programming and software engineering

In line with the survey, one of cyber security's leading "competitors" was programming/software engineering. This was predictable because the CCIT admission tests were centred around logic and programming quizzes and therefore catered to coders rather than young cyber security specialists. Around 40% of study participants declared that programming and software engineering were on the same interest level as cyber security and could be valid and appealing alternatives.

For example, one student declared that he would like to have either a career in cyber security or a job linked to programming, although he conceded that his plan

A was the latter. However, he had some requirements for his future job. He would not like to have the kind of job in which he sits at his desk and repeats the same tasks over and over. He would like to work in a team and undertake different projects. So, depending on whether his future job will have these characteristics or not, he will decide between programming or another sector, perhaps cyber security.

Another student said he was interested in cyber security but more on the “secure coding side.” He gave a score of 8 to cyber security and 9/10 to programming. He explained that he was interested “a little” in cyber security but more in “the practical side of programming because I like programming, but for the rest (cyber security), I have not had any particular experience.”

Similarly, another student gave programming a score of 9. She had been enrolled in several related courses during her bachelor’s degree and found that there was always something about them that excited her. She gave cyber security a score of 7/8 and said she was enthused by its “programming component”. At the moment, if she had to choose between the two sectors, she would opt for programming because it would give her more career options.

Another student had always thought of becoming a programmer one day. He was unsure about cyber security, mainly because he lacked information. He wanted to compare the two subjects and experiment with them. It is revealing that he decided to sign up for the CCIT because he initially thought it was a generic programming competition. One of the reasons he seemed more inclined to a career in software development was that: “I do not know what the average salary of a cyber security professional is, but I know that a good software developer who works for large companies has a good salary.”

Finally, a student did not see himself as a security expert, which he saw as having “something less” in terms of skills and opportunities than a software engineer. Instead, he thought he could become a software engineer with specific cyber security skills as he acknowledged that “competence in cyber security is always important for everyone working in the IT field.” He could not tell whether he would

have preferred a career as a “simple” software engineer or an engineer with cyber security skills, but he thought that a programmer with cyber security competencies had a leg up because they possessed skills in both domains.

7.5.3 CCIT influence on the relationship between cyber security and competing interests

An interesting question is the extent to which the CCIT was able to influence the interest of cyber security participants *in relation* to other competing interests. In other words, whether the CCIT could make a student more interested in cyber security than, for example, artificial intelligence if the two topics were approximately at the same level of interest before the beginning of the programme. This is difficult to assess with the present data, as information on competing interests were collected quantitatively only in the second survey, and therefore a pre-post assessment cannot be made. Nevertheless, the survey revealed some nuances between the CG and the TG (figure 40). In fact:

- 21% of TG participants said they would rather stay within the cyber security sector if they could. This was higher than the average population (16%) and higher than in the CG (13%);
- 50% of CG respondents declared they were interested in cyber security, but other topics and careers interested them at the same level, compared to 43% in the TG;
- 26% of TG students stated that they were interested in cyber security, but other topics and careers interested them more, compared to 29% in the CG;
- Interestingly, 10% of TG participants acknowledged they were not interested in cyber security, and they were unlikely to stay within this sector, compared to 7% in the CG.

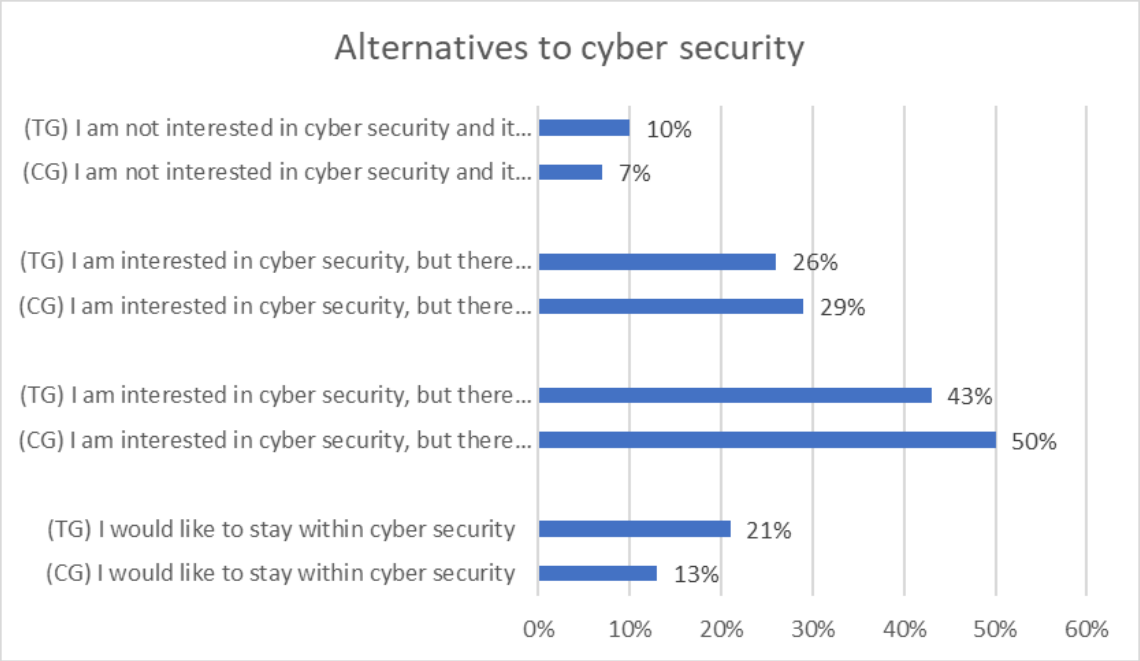

FIGURE 40

Interviews with TG students gave further clues. They shed light more on the complex interactions between competing interests rather than confirming whether or not the CCIT could sway participants in one direction or another. The paragraphs below present the six case studies of the TG students who were interviewed both before and after the CCIT.

When students were not very interested in cyber security in the first place, the CCIT did not make them change their minds. For instance, in the first interview, student 1 said he was not interested in pursuing cyber security compared to a career in artificial intelligence. In his second interview, he said his interest had decreased from 7 to 5, adding that he saw himself more in fields such as computer vision, image processing and machine learning. Similarly, in the first interview, student 2 declared he was not interested in a cyber security career, suggesting that ending up as a software engineer or in the finance sector was much more likely. In the post-interview, he said his (non) interest in cyber security had

remained stable, confirming that he was still interested in a career as a software engineer or perhaps undertaking a PhD in formal methods.

In a couple of case studies, the CCIT appeared to have had more of an influence, even though this did not mean that participants would try entering the cyber security sector immediately, mainly because of labour market issues and willingness to explore other professional areas. For example, in the first interview, student 3 was interested in a cyber security and an AI career. In his second interview, he said his cyber security career interest had increased from 7 to 8. However, because he had realized how difficult was to obtain an entry-level job in cyber security, he wanted to pursue a job as a software engineer first and then transition into cyber security, after accumulating some professional experience. Likewise, before the CCIT, student 4 was more inclined in an AI career. In the second interview, he reported that the CCIT raised his interest in a cyber security career from 6 to 10. Nonetheless, over the summer, he had formed an alternative interest in web development, which he was going to prioritize for the moment because of his new part-time job as a developer. Nonetheless, he added that he would have liked to switch back to cyber security at some point in the future because “in the end, the competencies that I acquire in development will help me in cyber security.”

In one scenario, the CCIT made student 5 realize that cyber security was the right career to lean on, even though he already had a well-developed passion for cryptography. Indeed, the student had already expressed interested in a cyber security career in his first interview, but not as much as in the possibility of doing academic research in cryptography. In the post-interview, however, his interest in cyber security as a topic and as a career had grown respectively from 8 to 10 and from 8 to 9. Moreover, he acknowledged that with the CCIT he “had moved much closer to cyber security than cryptography” and did not see any alternative to cyber security.

One case study was critical in showing how rapidly students might develop competing interests, even though they might have appreciated what the CCIT had

shown them about the sector. In fact, in the first interview, student 6 did not exclude becoming a cyber security professional one day but was more interested in becoming a programmer. In his second interview, his cyber security career interest had increased by 1.5 points. Yet, he did not see cyber security as his primary job goal because he had developed a greater interest in artificial intelligence over the summer. After his bachelor's degree, his future plan was to enrol in a more generic computer science-engineering or artificial intelligence master's degree.

7.6 Summary of findings

Chapter 7 sought to understand the extent to which the CCIT exerted any influence on its participants regarding important themes such as cyber security interest, educational and career planning, key choices and competing interests.

Section 7.1 found that the CCIT had increased interest in cyber security as a topic among the whole population. This is an interesting result as this occurred even among CG students, despite not being involved in the programme except for the admisson test. If one compares survey results among the two groups, more students from the TG declared the CCIT had significantly increased or increased their interest. During interviews, study participants generally stated that their interest had increased between February and October 2020. Not surprisingly, TG students explained that this increase was due to the CCIT, especially the training programme, a finding which will be reiterated and explained in the next chapter. Interest in cyber security as a topic among CG students had also grown, but this was due to a variety of factors, including the CCIT and the opening of new master's degrees and news coverage. These results are significant in the context of this research, which initially hypothesized that cyber security interest would have decreased among CG students and would have remained the same among TG students.

Similarly, section 7.2 discovered that the CCIT had increased interest in cyber security as a career in the whole population. An important finding was that the

CCIT had made interest in cyber security as a topic grow more than interest in cyber security as a career, confirming previous findings whereby topic interest and career interest do not necessarily fully coincide. The implication for a programme such as a NCSSC is that it should not be taken for granted that students will necessarily develop a vivid interest in a related career when undertaking a training programme such as the CCIT. In line with the results on interest in cyber security as a topic, while the increase in cyber security career interest among TG participants was mainly due to the CCIT, a variety of factors contributed to this increase among CG interviewees.

Section 7.3 discovered that students had little awareness of the cyber security sector, both in terms of educational offers and potential professional roles. In other words, despite a clear interest, CCIT participants were often unable to articulate ideas or plans on how they wished to bring this interest forward. TG participants seemed more likely to be more interested in specific educational and professional opportunities than CG students. This result is important as it helps us consider whether interest is a compelling concept and metric to evaluate policies such as NCSSCs in the context of skills shortages.

Section 7.4 gathered results on key education and professional choices that some participants made after the CCIT. Of the 110 respondents who changed their "student status" between September and October 2020, approximately half of them responded that the CCIT had partially influenced or influenced their choices. Furthermore, when comparing CG and TG students, the programme seemed to have a more prominent role in influencing key educational choices than decisions related to entering the professional world. These are also significant results that should be incorporated to better understand the impact of a NCSSC beyond the concept of interest.

Finally, section 7.5 aimed to determine whether CCIT participants had other interests than cyber security and how these "competing interests" relate to each other. Survey results showed that only a minority of students (16%) seemed to be completely devoted to cyber security. While interested in it, most students either

had other topics and career options that interested them at the same level (51%) or even more (25%) than cyber security. Artificial intelligence and generic programming or software engineering were the most popular among the alternatives. From survey data, it appeared that TG participants were slightly more inclined to get more involved in cyber security, even though interviews explained how dynamic relations among competing interests are and, therefore, the influence of the CCIT shall be considered unclear. These results are important and imply that even if an NCSSC could increase cyber security interest, this would not mean that interest in another topic or professional opportunity would necessarily decrease among participants. This should further help understand how to assess NCSSCs, which will be discussed in chapter 9.

8. The CCIT programme

Chapter 8 describes how the CCIT was enacted, highlighting the critical elements of the programme, including the admission process, training, skills challenges, and career awareness activities. This chapter answers the second part of the second main research question: How do NCSSCs influence participants' interest? What factors contribute the most to influence it? In doing so, it identifies the significant factors that are more likely to influence participants' interest and make a NCSSC "successful" in reaching this objective. This chapter does not seek to judge whether the CCIT changed participants' cyber security interest or not, which was the goal of chapter 7, but instead explores "how" it did so. This chapter is essential to understand the processes and context to consolidate and enrich the findings of the previous chapter.

It comprises the following sections:

- 8.1 presents the reasons that led students to sign up to the CCIT;
- 8.2 describes the impact of the admission process on students, especially CG participants;
- 8.3 is a deep-dive into the CCIT experience, elaborating upon various elements of the intervention, including the training, skills challenges and career-awareness activities;
- 8.4 summarizes the findings of this chapter.

8.1 Reasons for signing up

This section investigated why students decided to sign up to the CCIT in order to understand how these reasons related to their interest in cyber security. Students mentioned two main rationales: the willingness to increase cyber security knowledge and skills and the desire to compete with peers and challenge themselves. This section presents both survey and interview data.

Survey results (N=895) found that students signed up to the CCIT for the following reasons:[41]

1. To increase cyber security knowledge and skills (74.3%)
2. To get involved and be challenged (51.2%)
3. To understand what kind of professional opportunities there are in the cyber security sector (26.8%)
4. I am passionate about cyber security skills competitions (19.1%)
5. I am curious to try it (19.1%)
6. To get in touch with potential employers (7.7%)
7. To meet and get to know new people (3.4%)
8. Other (1.2%)

Interviews confirmed that students enrolled in the CCIT to take part in the training at the local university and the desire to challenge themselves.

For example, one student thought that the CCIT opportunity had come at the right time when she had started looking into a cyber security master's degree. She and her friends believed that it could have been beneficial to undertake the training to choose the right university course.

One student stated that the CCIT training could have been a chance to get deeper into the cyber security sector and obtain the skills required. As one could never stop learning in cyber security, the CCIT training seemed an excellent opportunity to see what the sector could offer and how it could enrich his cyber security knowledge.

The desire to compete and challenge other students was mentioned more often than the training, although by a very narrow margin. However, interviewees did not elaborate much on their logic:

> "… and I saw this as an opportunity to check what I am capable of, challenge myself."

[41] Respondents were allowed to choose up to 2 options.

> "To be fair, I enrol to challenge myself and to see whether I was capable of doing this type of things. Also, because, fundamentally, accessing the CCIT is something that regards logic, it involves programming. So, this is like a software engineering interview, so I said, let's see, let's get involved."

Interestingly, interviews did not reflect any career-related concerns. Whereas the survey found that many students were interested in attending to know more about professional opportunities (26.8%) and to be connected with potential employers (7.7%), this is something that interviewees did not mention.

Instead, a popular explanation was the desire among students to try "something new" and satisfy their curiosity, which was not necessarily and always related to cyber security. Rather, the CCIT was seen as an exciting event in the realm of computer science. For instance, one student declared that he tried the admission process because "primarily, it is something new" but also because he liked to learn anything that he did not know already about computers. Similarly, a fellow student from the CG mentioned that he had always been interested in the world of computers and computer science generally. However, he had not had the chance yet to understand enough about cyber security, and therefore the CCIT presented him with this opportunity.

Although the above were the most common reasons, interviewees mentioned others that prompted them to enrol, which are briefly listed here for the sake of completeness given the importance of the topic, but also because students clearly articulated why this was the case:

- *Fun/amusement*: one student said she applied because she liked puzzles. When she saw what the test entailed, she wanted to undertake it because she had fun doing those quizzes;

- *Networking*: one student wanted to attend because he wanted to get in touch with students who shared the same interest, which he deemed very important given how difficult it was to find like-minded peers. He argued that students interested in cyber security are more anonymous than others because, knowing how dangerous the online world can be, they try to defend themselves;

- *No cyber security pre-requisite*: one student thought it was important that the admission test did not request any a priori knowledge of cyber security. Given that the tests' pre-requisites were programming and logic skills, he enrolled and asked his friend to join as well;

- *Teamwork experience*: one student looked forward to entering a team and collaborating with other students. He explained that knowing how to work in a team was especially important in a professional setting, which is something that is not well simulated in a university environment;

- *Selective admission process*: one student declared that he had been teased by how selective the admission test had been, which meant to him that the CCIT was going to be a training programme where they were going to effectively teach him "something," contrary to the many free online courses that are trivial and not deep enough.

8.2 The admission process

This section aims to explain the influence of the admission process on participants, especially CG students. This is particularly important in understanding the overall impact of an NCSSC like the CCIT on students' interest. One hypothesis of this research was that CG students would have decreased their cyber security interest because of failure to be admitted to the training programme. As the previous

chapter demonstrated, this did not occur. This section explains why, including how CG participants found the test to be appropriate and their willingness to accept their momentary debacle to continue their cyber security skills development.

8.2.1 The appropriateness of the test

The admission test involved three phases:

- Online pre-test/selection, involving logic and programming quizzes;
- On-site morning test, involving logic and programming quizzes similar to those in the online pre-test but more advanced;
- On-site afternoon test involving a programming exercise.

The admission process was selective, as shown by the number of students admitted to each phase in the table below:

TABLE 19 ADMITTED STUDENTS TO EACH PHASE

Students who signed up online	Students who took the online pre-test	Students who passed the online pre-test and sat the online pre-test	Students who passed the morning test and took the afternoon test	Students admitted to the CCIT
4,454	2,760	1,869	1,448	560
Admission rate	62%	42%	33%	13%

Students enjoyed the presence of logic quizzes in the online and morning tests because it allowed a broader pool of individuals to participate, for example, those

without a strong programming background. However, despite letting a wider audience attend, interviewees appreciated that the tests were complex enough so as to not guarantee an “easy pass.” Moreover, students believed it was important that the CCIT had tested logical skills. One student from the treatment group admitted that, in the beginning, it was not clear to him why logic quizzes were so pervasive in the tests, but after starting the CCIT, he realized that one needs logic skills to tackle cyber security skills competitions.

Students from both the CG and TG reflected that the last part of the admission process had been particularly challenging and, for many (especially high school students), beyond their extant skills.

One student from the CG declared that the afternoon test had been “a disaster” to the extent that she had to withdraw halfway. While she had always been interested in programming, she had never studied the kind of programming required in the afternoon test: “I took a look and said [to myself], very simply, I have never done these things, I have never had the time, and thus I said [to myself] (…) I should go home and study for my chemistry exam…”. Another student from the CG said that the programming exercise could have been particularly challenging for high school students, as it involved mathematical concepts that were not typically included in a high school curriculum.

This feeling about the afternoon test was generally shared also by TG students. One interviewee described the admission as “relatively tough”, noting that especially the afternoon test had been challenging, with many students who had left the testing site after only 10 minutes, as they had no idea how to complete it. Another TG student agreed that the afternoon test, while effectively measuring programming skills, had questions on knowledge and parameters, such as the efficiency of the algorithm running the programme, that one would face in pure programming competitions.

The nature and difficulty level of the afternoon test led to an interesting debate regarding the overall appropriateness of the admission process. On the one hand, a minority of interviewees (34%, 10/29) expressed some scepticism about the afternoon test. What is interesting about this minority is its composition: 30% (N=3) belonged to the CG, and 70% (N=7) were from the TG.[42]

For example, one student who had followed formal cyber security courses at university and attended several skills competitions was doubtful about the ability of the programming exercise to assess students' suitability to become good cyber security practitioners. He said that the afternoon test was literally a coding test, but being good coders "does not mean being good [in cyber security] (…). Well, yes, it is required knowledge but not sufficient in my opinion." I asked him whether what was usually requested in other cyber security skills competitions was very different than what was found in the CCIT admission process, and he answered, "Yes, yes, absolutely." He explained that, in cyber skills competitions, the most complex exploits[43] do not require more than 40 lines of code; a good coder cannot necessarily fix these issues, and advanced knowledge of algorithms is helpful only to a limited extent. He made an example of the best security teams in Italy, which usually do not aim to optimize algorithms when they have to write a script to launch an attack. What is really required is an accurate knowledge of a language, computers' inner workings and the whole IT infrastructure. He concluded that he would not necessarily know the best way to select the right candidate, but the current one was not entirely correct in his opinion.

One student declared that the topics used in the admission test were not relevant and did not mirror what the CCIT training programme entailed. While he admitted that logic and programming were elements that are part of security competitions:

[42] This implies that more than half of TG students (54%, 7/13), who later gained a rounder understanding of cyber security through the CCIT training, thought that the admission process had not been the best instrument to find the right candidates to attend the CCIT.
[43] "An exploit is a code that takes advantage of a software vulnerability or security flaw" (Trend Micro, n.d.).

> “they did not regard security; therefore many people accessed [the training programme] without knowing what they were going to face. In my opinion, [the admission process] should be a little bit more focused, so perhaps have an admission process with some basic cyber security concepts.”

On the other hand, most students from both groups (66%, 19/29), and in particular most students from the CG (81%; 13/16), considered the test to be appropriate. Their main argument was that they saw both logic and programming skills to be the “classic” requirements of any computer science contest and the foundation for anyone aspiring to become a cyber security specialist:

> “Yes, I would say so (i.e. whether the test was appropriate or not), because in the end, those are the required competencies to start working in cyber security, (…) having programming skills (…) and logic are the pivotal points.”

This is an important finding as the appropriateness of the admission process is one of the factors explaining why CG students’ failure to be admitted did not decrease their interest in cyber security, contrary to what was hypothesized by this research. This is, for example, what happened to one study participant, whose interest plummeted from 6 to 3 (see table 17), and whose case is particularly relevant to illustrate the logic of the initially stated hypothesis.

This student was particularly vocal about the admission test and was very upset about the outcome. In his opinion, the main reason he had not advanced was that he was a lyceum student. It was evident, he argued, that students from technical schools had had an advantage compared to students from lyceums, most notably because technical institutes better prepare their students in practical subjects such as programming (the central requirement of the final stage of the admission process). Thus, when CCIT organizers communicated the final score, he received the result with sarcasm and concluded that “if [the CCIT] was looking only for those who could do some little trivial programming, I am not the right person, what can I

say." He said that failure to be admitted was a real pity because his interest in cyber security could have significantly changed:

> "[My interest in cyber security] could have increased much more; in fact, it could have become a job prospect if [the CCIT] had gone well, I would not have chosen to study economics (i.e. next year), and I could have chosen computer science or computer science-engineering; I would have changed [my orientation] if [the CCIT] had been a surprise."

His case study is interesting as it exemplifies what this research hypothesised was going to happen for most students not admitted to the training, namely disillusionment following the outcome of the admission process, which would have sapped their cyber security interest. However, most CG felt the test was appropriate, and their failed admission did not decrease cyber security interest. The following section clarifies what other motives may explain why the admission did not negatively influence CG participants' view of the CCIT and cyber security in general.

8.2.2 CG participants' feelings about the admission outcome

While all CG students were disappointed about the test outcome, their admission failure did not translate into bitter feelings towards the CCIT and cyber security. One of the reasons this did not happen has already been revealed above: students in the CG largely thought the admission test was appropriate. However, this was not the only explanation: students showed acceptance of the outcome and recognized they came to the event unprepared; they had low expectations; they were pleased by the introduction of the OCCIT; and knew about the high competition in certain local universities.

A theme that strongly emerged was students' acceptance of their "failure" and their willingness to persevere in this endeavour. This was highlighted when they discussed how they saw their interest in cyber security evolving after the CCIT. In a way, they saw the admission debacle as a normal part of their skills development process, which could entail facing different obstacles before reaching the objective.

Interviewees showed grit and an unexpected level of determination in choosing not to give up.

Whilst particularly disappointed in the outcome, one student started searching for online cyber security courses after finding out she had not been admitted. She and her friend knew it would have been difficult to pass the programming exercise given the intense competition, and they were happy that they had at least tried. She added that they did not feel discouraged about the negative results and that they were going to try again the following year: “we do not give up; we are not that kind of girls.”

One student was content about the experience and confirmed he would reattempt the test next year because “it was very nice and made me think.” He said that disappointment did not prevail because one has to learn from everything, from both wins and losses, and in case of a loss, one should have the courage to try again: “one needs to roll up its sleeves, try again and learn.”

One student asserted that the admission “could have never taken away my desire for cyber security.” He declared that if one wants to achieve something, one needs to fail 100 times. Trying only once and achieving success perhaps does not even make one taste victory properly because nothing happens like that: “One needs to suffer a bit and work hard.” So, one might suffer a defeat, but it will help one find his/her way and the right motivation.

Other reasons explained why students, while dissatisfied about the outcome of the admission process, did not feel it should have lowered their interest in cyber security:

- *Unpreparedness*: one student was saddened because he had not been able to live up to his expectations in the programming exercise rather than because he had not been accepted to the training programme. A similar feeling was shared by another student who said that he was expecting a negative result as he had taken the test too lightly. Hence, he had been

frustrated more at himself for his inability to plan in advance rather than the negative outcome. However, both students confirmed that this did not discourage them from pursuing their cyber security interest further.

- *Low expectations*: a couple of students reflected that the failed admission was expected as they attended the event mainly for fun and therefore did not really foresee being accepted. In this context, one student said she was already eyeing the next admission process in January 2021: “I thought about signing-up again because I liked the experience, the admission tests, now (…) perhaps I can get involved more seriously and not trying for the sake of trying it.”

- *The OCCIT*: another student was aware that the afternoon test did not go well and was expecting to be excluded from the training. While he had been upset about the result, he had enrolled in the OCCIT, which had allowed him to know more about cyber security.

- *High competition*: a student was clearly upset about the outcome, especially given how invested he was in cyber security. However, he took the results philosophically, reflecting upon the high competition. He knew it would have been difficult to finish in the first 20 positions in Milan, which usually attracts a higher number of candidates than other nearby universities. He distinctively remembered thinking that there were going to be students who “must have spent their life doing those types of tests” and who were going to be better than him. In the end, he was happy he had reached the afternoon test stage. I asked him to what extent this had an impact on his interest, and he claimed it had not changed anything because he was already too involved in cyber security to abandon it.

To conclude, one quote from a student very well summarizes the overall mindset of CG students about how they felt regarding their non-admission:

> "Well, I was upset a little but, but not even too much because I knew. When I saw the test, I thought that I could not do it and therefore I was expecting the afternoon [result], but my interest did not go away because in the end, you cannot always win. (…) I cannot do these problems today, but maybe I will be able to do them in a year when I will have more experience. [However] It was gratifying a bit because I got myself involved in something I could not do, but I liked it, I had fun for a day. I liked it, I liked the contest."

8.3 Inside the CCIT experience

The CCIT programme took place online between March and October 2020 and consisted of a 3-month cyber security training, the June local skills competition, the October national skills competition, and career-awareness activities. This section aims to identify and explain in-depth which factors influenced TG participants' cyber security interest during the CCIT programme.

The main finding is that students particularly appreciated the new cyber security knowledge and skills they acquired through the training, even though the online delivery due to Covid-19 limited its potential.

8.3.1 The CCIT training

8.3.1.1 Training content and delivery

When students were asked to name the most positive aspect of their CCIT experience, there was one clear winner: the new cyber security knowledge and skills they gained during the three-month cyber security training, which occurred between March and June 2020. Students cherished the fact that the training went

in-depth and was practical at the same time, touching upon topics that they would not have learnt by themselves.

Students particularly appreciated the level of knowledge and skills they acquired during the training, particularly receiving a good level of foundational knowledge, the breadth of topics and the practical components. The CCIT training programme comprised of the following topics, which were delivered online through a blend of theoretical classes and lab-based activities:

- Introduction to cybersecurity
- Attack/Defense
- Cryptography
- Hardware security
- Network security
- Software security
- Web security

The first element that students noticed was how satisfactory the training had been in teaching foundational cyber security knowledge. One student assessed that teaching core knowledge was essential, especially for those participants without a cyber security background (the majority). Along the same line, another student said he had been satisfied with the information he had received as he had used it to get deeper into the subject on its own.

Furthermore, students appreciated the variety of topics the training touched upon. For example, one interviewee reflected that it had covered many theoretical aspects of cyber security in-depth and their practical components as well. He commented that the training had been helpful to get deeper and to deal with many topics he would have never been able to tackle alone. Likewise, a student explained that they had engaged with an “ample spectrum” of subjects, ranging from number theory to specific security protocols. While this broad introduction was helpful, he also appreciated the possibility of specialising in specific topics.

In addition to teaching core knowledge, students enjoyed the practical component of the training. One explained that there had been a good focus on cyber security practical applications. A fellow student added that the nature of the training, a mix

of theoretical lessons and lab-based assignments, meant that the skills programme had been more engaging than the usual university course. Some students provided specific examples of how practical the training was. For instance, one student argued that thanks to the CCIT, he learnt various techniques to scan for vulnerabilities and exploit some of them using tools such as CyberChef or the Burp Suite.[44] In another example, one student had been excited to learn about web security: “one of the most important things that I have learnt is to tinker, let’s say so, try to break things on websites.” He also learned to reverse engineer software, which he did not know prior to the CCIT, allowing him to practice what he knew about computer architecture.

Despite the overall positive training experience, students highlighted two drawbacks: timing and difficulty level.

At least a couple of students mentioned that the training timing could be improved as most of it took place during the university exam session. The consequence of this overlapping was that students had to dedicate time to both regular studying and the CCIT training. So, students had difficulties dedicating the right amount of time to the CCIT. One student suggested that the CCIT should consider pushing the training into the summer, transforming it into an “internship” of one or two months.

Other students mentioned that the training difficulty was high, and there was pre-requisite knowledge that instructors should have taken the time to explain, especially to the younger participants. According to them, the training had been designed with university students in mind, which meant they had to put in some extra time and effort to understand more advanced concepts. For these students, this represented a challenge they had been willing to face, but it had been problematic, at least initially.

[44] CyberChef is a web app for carrying out all manner of "cyber" operations within a web browser (GCHQ, n.d.). The Burp Suite Professional is a popular penetration testing and vulnerability finder tools, and is often used for checking web application security (Delta Risk, n.d.).

8.3.1.2 Relationship with professors

The relationship with professors and the tutors involved in the training (i.e. PhD students, post-doctoral researchers or former CCIT alumni) was one of the elements that CCIT participants appreciated the most about the programme.

Students recognised the high expertise of their instructors, with many interviewees defining them as “competent” and capable of explaining well the most important elements of the course. For example, one student considered his professors to be “extremely well-prepared” to the extent that they had gained much of his “trust and respect.”

Moreover, students enjoyed the educators’ willingness to satisfy their curiosity, sometimes even outside regular teaching hours. One student explained that his instructors had been very supportive and highly responsive to all the additional questions, going even further in being available “for every question, 24/7.” One student reported that his professors used to organize a small competition every week, providing advice and training even during weekends: “even when they were not on duty, they were having fun with us (…) teaching even outside the normal class hours.”

Students often talked about a more relaxed relationship with professors, especially compared to the usual physical university setting. Indeed, many (university) students already knew their instructors as they were enrolled in higher education courses delivered by them. For instance, one participant noted that professors “behaved more informally compared to a university class, so it was nice.” In a similar vein, one student suggested that the training had had the benefit of pushing the boundaries a bit, “going beyond the usual professor-student relationship; they were very helpful and active during our journey.” Finally, one student noted that the relationship with professors went exceptionally well as far as saying that “more than instructors, they became friends, colleagues, because they were very helpful in answering questions they did not really know.”

8.3.1.3 Relationship among students

While students were pleased by their relationship with the instructors, the assessment of the one with fellow students was mixed. One can argue there have been two types of experiences: a very dynamic one, where the idea of the team was shared among participants, and a more detached one.

Approximately 30% of TG students suggested that their relationship with fellow students had been very satisfactory. One student, for example, said that the lab assignments had been beneficial to "form a nice group." These lab assignments usually took place during weekends, "when from 3 pm we started programming until 7 pm and then those who wanted could stay longer." He stated that the added value of the lab assignments was working in randomly created teams, meaning that one did not necessarily end up with a friend, but most of the time worked with someone one had never worked with. These tasks had been instrumental in doing some networking. He added that the professors had created this nice social dynamic ("they cared a lot about the creation of a nice group"), and their ability to leverage the social component of the training established a "productive competitive dynamic."

Another student confirmed that instructors had a prominent role in creating a fruitful group dynamic. They used to organize a small competition every week, organizing small teams and helping them through the task:

> "It was really an unrepeatable experience that I will keep forever…even now, from time to time, we gather with the old team members to take in part [in competitions] as we used to do until some months ago."
>
> "And even then the collaboration which we could have among us in the team, one could really…it was something unique."

However, most interviewees (approximately 70%) did not seem to have had such profound and collaborative social dynamics, with many students lamenting that the

online delivery of the training created detachment among participants. An explanation from one student summarizes very well the experience of many:

> "[The relationship with colleagues] I should say it almost did not occur because we were following classes in front of a screen; it was practically non-existent, except with the colleagues from university with whom I already had a relationship."

A couple of students explained in more detail why their relationship with fellow trainees did not grow. One student stated clearly that social dynamics "were limited by the pandemics." He said he did not have the chance to know the rest of the students because he had never met with them, "having seen only their online picture, for those who had it…it was not easy to create a relationship." In the end, he was able to build some stronger ties, but only with a couple of students with whom he attended the final national competition in October 2020.

Another student explanation was interesting as he compared his experience with another competition he had been part of in the past. He said that because all the training moved online, these virtual classes had not been as "warm" as he had imagined them. He recalled the experience leading up to another competition, the Rome Cup, where he and his peers used to study together. He remarked the stark difference with the CCIT training, where they were instead separate and "which lead to a detachment." He thought that this experience did not make him feel part of a team, which would have happened if they had been in class together.

8.3.1.4 The impact of Covid-19 on the CCIT training

Considering these findings, students were asked how their training experience would have been without Covid-19, and the answer was almost unanimous: it would have been much better.

A couple of students had milder views and believed that the online format had some benefits. For example, the online delivery had cancelled any distance and commuting issues. Moreover, according to one student, online training could

substitute 70-80% of face-to-face teaching even in “normal” conditions if it was well managed by professors. However, his views had been influenced by his own experience, which his instructors had made highly interactive.

This notwithstanding, every student in the TG agreed that Covid-19 had negatively impacted the social and human component of the training to the extent that, according to one student: “[the training] would have been much better, it would have been something totally different…not that this was negative, but in my opinion, the human contact was missed by the professors and also us.” On-site training would have had several benefits, including:

- More collaboration among students and less individualism
- Deeper social bonds, perhaps leading to friendships
- More dynamic and interactive lessons

In a related question, students were asked to name one negative aspect of their CCIT experience, and most of them mentioned the online delivery imposed by Covid-19, which confirmed the above finding that the online environment limited the training’s potential.

8.3.1.5 A case study of a bad training experience

Despite being delivered online, TG students were satisfied with the training, except for one participant. His case study is crucial as it is one of the only two students from the TG who reported a decrease in cyber security interest following the training (see section 7.1.2). His experience is valuable as it confirms the key elements that should be considered in a training for it to be successful, namely the quality of the teaching and the interaction with instructors and peers.

The first element that the student highlighted was related to teaching. He immediately noticed that the training had to move online, given the health emergency. Nevertheless, rather than the online nature of the training per se, what bothered him was how the instructors used the online medium to deliver the

learning experience: “often professors would refer to the online lectures on the platform and then we had to do the challenges on our own.” He seemed to imply that professors let the video lectures on the platforms perform the teaching job they should have done. Furthermore, he thought the online lectures were disconnected from the online skills challenges they had to undertake, noting that he had to spend much time searching for answers that the slides used in class were unable to give. He stated that the additional learning he had to do to complete the challenges had been “very invasive.”

Regarding his relationship with the instructors, he described it as almost non-existent because interactions had been limited. Similarly, the relationship with classmates had been slightly challenging due to the competitive environment the training had created. He explained that the skills challenges were thought to give a score which contributed to the final raking of the June local challenge. This created a competitive dynamic among participants, with some of them refusing to collaborate as “they were only concentrated on their victory.” However, it seemed that this approach was taken only by his university, among all the interviewed participants.

8.3.2 The skills challenges

An integral component of the CCIT programme were the local and the national cyber security skills competitions, which had to be moved online because of Covid-19.

The local skills challenge took place in June 2020, and it acted as the apex of the three-month training. All students who had attended the training were automatically admitted to the event. The June challenge was “local” because each participating university organized it and because participation was limited to those students who had trained at that specific university only.

The national skills challenge occurred in October 2020 and instead saw the participation of a team of selected students from each university: six students were selected based on the final ranking at the June local challenge.

As critical components of the whole programme and a national cyber security competition in general, this section assesses the impact of the skills challenges on students' experience. The main finding is that students enjoyed the local skills competition but had a more negative experience in the national one. However, both events did not influence their overall assessment of the CCIT as much as the training did.

8.3.2.1 June local skills challenge

The June local challenge consisted of a seven-hour Jeopardy-style skills challenge,[45] which included questions with varying difficulty levels in various cyber security topics (web security, cryptography, hardware security etc.). Overall, students enjoyed the event, with some of them being enthusiastic about it:

> "The experience was really unique because I had personally taken part in other skills competition in those months, but I had never been in a skills competition of a seven-hour duration."

Among the positive aspects, students mentioned the possibility of putting into practice what they had learnt during the training. Most importantly, they felt that the training had prepared them well for this kind of challenge: "I think that without the training I would have scored very fewer points; instead (…) I was able to achieve a good score, which I am happy about." Furthermore, because the challenge included various tasks at various difficulty levels, students could choose the tasks they enjoyed the most.

[45] A jeopardy-style cyber security skills competition features a number of fixed problems with pre-assigned scores in a range of cyber security domains. The winner is the person or the team that scores the most points (Eagle, 2013).

Students did not report any significant drawbacks about the local challenge. They highlighted that the event did not raise any significant issue from a technical perspective. However, they mentioned some aspects that could be taken into account in the design of a national cyber security skills competition:

- *Nature of the challenge*: three students reflected that they would have preferred to work through the challenges as a team. They lamented that they could not discuss the tasks with classmates. One student said that: "The fact that we had to work individually, I think it penalized me a bit, and I did not feel adequately exploited." However, it should be underlined that the choice of making this skills challenge individual was due to its nature as a mechanism to select the students who would then attend the national skills challenge.
- *Timing*: similarly to the issue of the training timing, a student mentioned that when he realized that some of the tasks would have been too difficult to solve, he had to leave the event to study for a university exam.

In the end, however, while students were generally satisfied with the experience of the June local skills competition, no one specifically mentioned it as the main positive aspect of the CCIT programme, as instead, they did for the three-month cyber security training.

8.3.2.2 October national skills challenge

The October national challenge consisted of a day-long attack-defence skills challenge,[46] where each team controlled a remote host linked to a virtual network. The remote host provided services that were managed by a server controlled by the CCIT. These services had been coded and implemented to contain security flaws, which each team could exploit in order to gain points. A total of 168 CCIT

[46] An attack-defence is a type of cyber security skills challenge in which participants have to manage a network with vulnerable services. A team should patch its own services while finding vulnerabilities to hack into other team's networks (Eagle, 2013)

participants attended the event, including six interviewees from the TG who were able to discuss the main positive and negative aspects of the event.

Students had a different experience in the national competition than in the local one. While students appreciated the novelty of such an event, they also felt they had been largely unprepared to face competition's tasks. Interviewees generally believed that the training they undertook was better suited to tackle jeopardy style competitions rather than attack-defence ones, with the consequence that some of them did not know what to do at the beginning of the challenge. Students gave different explanations why they had felt they arrived at the main event of the CCIT programme undertrained.

One was related to the postponement (from July to October) of the national skills challenge due to Covid-19. A student explained that this had diluted interest in the final event to the extent that, even though the delay meant more time to train, this extra time had not fully been used. This occurred because, following the end of the training period, instructors had other commitments and were usually less available to provide training suggestions.

Another explanation was the poor organization and communication of some local universities. One student bitterly commented that “there is little to say here because we were really left to chance.” He was “very disappointed” because, while they knew a final national competition would happen, no one from the university communicated how and when this would occur. Only in September, two months after the local competition, did they receive a message from one of the instructors stating that the competition trials were going to take place in two days. The student were bewildered by the lack of communication, and this sentiment was enhanced when they saw the content of the trials, which made them realize they were not well prepared for the challenge. After the trials, they still received no training and “we only waited for the day of the finals.”

Another possible explanation was that, at least in some universities, instructors were not fully prepared to deliver the right kind of training for this type of challenge. For example, one student said that, while his instructors had been highly competent and helpful, they did not have much experience in attack-defence competitions. In contrast, he noted that many of the teams which ranked in the top eight spots had been trained by instructors who had previous experience in that kind of attack-defence competition.

In the end, however, while students were generally dissatisfied with the experience of the October national skills competition, no one specifically mentioned it as the main negative aspect of the CCIT programme, which instead was the online format of the training.

8.3.3 CCIT and careers

One of the most important aspects this research investigated is how the CCIT could influence interest in a cyber security career. This section reports on the career-awareness seminars and activities that the CCIT organized and attempts to gauge their influence on students. Participants had mixed reviews about these activities, whose practical impact is hard to assess with the current data.

Students mentioned that the CCIT organized cyber security career awareness seminars to advance participants understanding of the sector. From students' accounts, it seemed that the organization of these events had been devolved to each local university, rather than being centralized, with the result that students' experiences tended to vary significantly.

Generally, local universities organized seminars with local sponsors. For example, one student recalled a meeting with Exprivia,[47] whose representatives had given multiple examples of how cyber security was embedded in their business

[47] Exprivia is a company specialized in software development and the provision of other IT services (Il Sole 24 Ore, n.d.).

operations. Another student said his class had a meeting with a company called Telsy,[48] which showed real-world cyber security applications.

In other universities, it seemed that instructors took the lead in showing cyber security professional applications. For example, one student explained that for each topic, there was an overview of the state of the art regarding the subject, including an explanation of security professionals and tasks involved.

On the other end of the spectrum, one student reported that neither private companies had made presentations about their workflow nor their instructors had described cyber security professional applications. Even if their educators had done that, he was sceptical about what evidence they could have brought: "(…) it was not even mentioned what one could do after (as a cyber security job). Also, because the instructors were professors or PhDs, thus people who had never worked in this sector, therefore I think they would not have known what to say."

Students had mixed reviews about the careers seminars. For a couple of students, these meetings with private companies had been helpful in several ways. One interviewee understood what key cyber security professional figures were there and learnt what a security operations centre did. He was more familiar with firms' approaches to cyber security and how the workflow in some sectors was organized. Because of that, he wished there had been more than a couple of these professional seminars. Another student reflected that career-awareness efforts had been valuable to clarify his ideas about professional cyber security and how to "combine everything."

For some other students, by contrast, these seminars did not mean much, with some quotes from students illustrating well their apathy:

[48] Telsy is a company operating in the industry of telecommunication protection and cybersecurity (Telsy, n.d.).

> "From what I remember, there were some seminars (…). I followed one, I think, but I cannot remember well which private companies or how many."

> "There were lessons, how to explain, that were connected to the real world (…)
>
> *(Researcher) Did you talk about careers as well?*
>
> No, I do not think so."

> "Yes, for example, the sponsors' presentations, if I am not mistaken, they also made us understand in which sector the cyber security role is in demand."
>
> *(Researcher) What do you remember about those presentations?*
>
> I cannot remember (anything) right now."

According to one student, these professional seminars backfired, at least for him. In his opinion, these meetings had been organized with the intent to sponsor and publicize companies rather than provide useful information. He did not appreciate this and thought that some organizations came to those seminars to show how nicely they were doing their work and to "use big words." He believed this had been unhelpful given that the students were not necessarily looking for a job.

In addition to these seminars, the CCIT attempted to create closer ties with the professional world by asking participants to upload their CVs onto the CCIT platform so that companies could contact them. Even in this case, though, the impact of this initiative was mixed. At the time of the second round of interviews (October 2020), approximately half of TG participants had been contacted by firms. Nevertheless, the immediate impact of the interaction with the professional world was not clear. Although students did not necessarily perceive it as such, the main issue was the timing of the interaction, with interviewees often looking to complete

their studies rather than for employment. Therefore, most of the time, the outcome of companies-to-students interaction was the possibility of students undertaking their thesis with the company.

For instance, one student had been contacted by two firms, but he had made immediately clear that he intended to continue studying (in October 2020, he had started his master's degree). Therefore, the two companies did not offer any placement, although they suggested keeping in touch because "in the future, there could be internship opportunities…or open positions that I could be interested in. And so, I consider even this type of interaction as something positive."

In a similar vein, a student had been contacted by Accenture, an interaction which he deemed as "useful." For the moment, they had decided to talk no further about a possible placement "because I have no intention to start a professional career before finishing university." However, he was pleased that the company had suggested writing his thesis with them and having another meeting the following summer (i.e. 2021) to discuss placement opportunities.

In this context, the experience and scepticism of one student were particularly illuminating in highlighting the broader issues that might be affecting the interaction between cyber security skills supply and demand. He narrated that a representative of IBM came to give a presentation about the cyber security sector, particularly referencing how the sector is in dire need of personnel. However, the student experience with the labour market so far had given him a different impression:

> "This is something [the availability of open positions] that I cannot see when I go and look for opportunities, I don't know. That is, this is (a cyber security job) something they talked about like is something easily accessible, like there are many positions etc, but probably the best offer that you can receive is an unpaid internship (…). So, yes, they showed what it is possible to achieve with a cyber security career, but in my opinion they did not concentrate enough on how to start…because the end point is clear to

everyone, you become a cyber security expert and you earn a lot of money. (But) The starting point is not very clear."

He claimed that if he wanted to be serious about his chances to obtain an entry-level cyber security job, he would need to do more personal projects in cyber security or get some sort of experience. He was unsure about what the CCIT added in this regard: "I cannot put the CCIT [on my CV] and pretend that companies like Mozilla would be interested in my profile because I did the CCIT…the CCIT is useful on a personal level, but it is something that does not add too much value on a CV anyway." He somehow wished there was a solution to his difficulties in entering the cyber security labour market, and he attempted to give one. He theorized that companies should have some security-specific training programs where interns could test their cyber security knowledge in a simulated environment. It would be essential to have this simulated and gamified approach because "obviously you cannot give a [IT] system to a new grad and make him/her manage its security because there could be lives or money at stake, you cannot do that."

8.4 Summary of findings

Chapter 8 aimed at unpacking the main factors that influenced participants' interest in cyber security during the CCIT. In particular, it focused on two main elements of the national competition, the admission process and the training programme. The goal of this chapter was to highlight "how" cyber security interest changed rather than "the extent to which," which was the main objective of the previous chapter.

Section 8.1 explored the reasons behind the students' decision to sign up to the CCIT. The main explanations were their desire to challenge themselves in a new activity and to receive cyber security training, which they saw as an opportunity to increase their knowledge of a new field.

Section 8.2 delved deeper into the CCIT admission process. This section is critical in helping to understand the influence of a national cyber security skills competition

on students who wanted to attend but who were not admitted. Indeed, this research initially hypothesized that the outcome of the admission process could have had a strong influence on participants' cyber security interest. There was general unanimity in considering the test both fair and difficult, especially the decisive afternoon test. Most students in the CG thought the test was appropriate. Because of this, and other relevant reasons, students in the CG did not see their failed admission process as a strong enough motive to give up on their cyber security interest or the CCIT. Instead, a theme that emerged strongly was their acceptance of the negative outcome and their willingness to move forward and learn from their mistakes.

Section 8.3 was a deep-dive into the CCIT programme, which included a 3-month online training, local and national skills challenges and various career-awareness initiatives.

The training and the related cyber security knowledge and skills that students acquired were the most positive aspects of the CCIT. Students particularly enjoyed receiving good foundational knowledge, the breadth of topics and the practical lab-based components. Interviewees also appreciated the expertise and the helpfulness of instructors. On the other hand, they were generally dissatisfied with the relationships they were unable to forge with their classmates due to the online delivery of the training, described as the most damaging aspect, even if they were aware this had been due to Covid-19.

Students gave very positive reviews of their experiences in the local challenges. Overall, everything proceeded smoothly from a technical standpoint, and they felt that the training had given them the right intellectual and practical tools to undertake the challenge. On the other hand, the fewer interviewees who had been selected to attend the national challenge were not particularly satisfied with it as they believed they had come to the event unprepared. In the end, however, the three-month training was more important than the challenges in influencing their assessment of the CCIT.

Students were also involved in career awareness activities, namely seminars with private companies and uploading their CVs on the CCIT platform. Overall, it is harder to understand the modalities and the outcomes of these activities as students accounts of these interactions were mixed. Students have gained some knowledge of cyber security careers, but not too comprehensively; some obtained the possibility to research their thesis in some companies, but not more concrete job placements. Regardless, students were more enthusiastic about the CCIT training than career awareness activities when assessing their CCIT experience.

9. Is an NCSSC an effective solution to help mitigate the cyber security skills shortage? A discussion

Taking into account the literature review (ch. 3), the hypotheses (ch. 4) and the results of this thesis (chs. 5-8), this chapter aims to discuss the role of national competitions as an effective public policy in the context of the skills shortage.

This chapter argues that a NCSSC organized and implemented like the CCIT could be an effective policy tool to curb the shortage as it helped trigger and increase cyber security interest among its participants. In doing so, it is well-placed to make students more likely to consider cyber security degrees and careers, of the major issues currently worsening the shortage. Nonetheless, this chapter also contends that a NCSSC could have an even more prominent role if:

1. It is part of a broader cyber security development system. A NCSSC could become the cornerstone of such a system if it manages to “meaningfully engage” all the participants it recruits. This system may also foresee the inclusion of formal cyber security coursework in secondary and higher education curriculums. However, this system is unlikely to work unless employers cooperate in developing a national pipeline of young cyber security professionals.
2. It maintains high standards of cyber security training and elevates cyber security career awareness activities to the same level. As it is difficult to shape career decision-making and choice, these activities require the same expertise, resources and time as cyber security training and skills challenges.
3. It integrates other relevant outcome variables, most notably educational and career planning, key career choices, and “competing interests” to correctly assess its influence. However, NCSSCs should retain *interest* as one of their outcome variables as it is more easily achieved and still constitutes a good indicator of how participants assess the programme and view cyber security.

It is essential to underscore that, on its own, a NCSSC is unlikely to achieve what a concert of policies might in dealing with the shortage. As the issue has several roots, there are limits to what a NCSSC can do alone. Nonetheless, if such an intervention could effectively help trigger interest and positively influence it, it would lay a strong foundation for other policies to further steer students into the cyber security sector. Thus, this chapter suggests looking at the shortage holistically and, when resources allow it, having a comprehensive policy response.

Furthermore, this chapter discusses this thesis' contribution to interest theory, including how it:

1. Provided content-specificity, identifying the primary triggers that elicit cyber security interest. However, these triggers may also fuel interest in other subject areas.
2. Found that participants differentiated between interest in cyber security as a topic and as a career. This implies that more research should be done to understand when vocational interest emerges as a result of interest development in a specific topic.

This chapter analyses all these topics, although not necessarily in the abovementioned order.

9.1 Contribution to interest theory

As this thesis investigated NCSSCs through the concept of interest, it contributed to theory in two ways.

First, it added content-specificity to the theorization of interest development, identifying the triggers of cyber security interest, a theme that had not been researched before. Hence, the first part of this section maintains that curiosity is a

crucial element in eliciting interest, and there should be further exploration of how engaging with it could better serve the development of cyber security interest. Moreover, findings highlighted the role of the CCIT as an interest "generator," suggesting that if a NCSSC has the potential to trigger interest, stakeholders should focus on how to make their public affairs and marketing strategies even more wide-reaching.

Second, this research also sheds some light on the relationship between interest development and vocational/career interest. Thus, the second part of this section argues that the relationship between interest development and vocational interest should be further investigated, especially determining at which stage vocational interest emerges.

9.1.1 Triggers of cyber security interest development: the role of curiosity and the CCIT

This thesis's first contribution to interest theory was on content specificity, as it is perhaps the only study that thoroughly explored the concept of interest development through the lenses of cyber security. Specifically, it provided much-needed evidence on the interest triggers of those individuals who are particularly relevant for a country's cyber security workforce, namely NCSSC participants. The research found three primary triggers: general curiosity in the topic, formal and informal coursework, and the CCIT itself (section 5.2). In this section, I discuss the role of curiosity and the CCIT, whereas I talk about the importance of including cyber security coursework in the next section.

According to survey and interview data, curiosity was important to develop what Renninger and Hidi (2006) would probably describe as situational interest in cyber security. This is an important finding, hinting at the debate on the relationship between curiosity and interest development. While researchers such as Schmidt and Rotgans (2021) argued that there is no difference between epistemic curiosity and situational interest, Hidi and Renninger (2020) instead pointed out that such a

difference exists, despite the two concepts sharing some attributes. Curiosity involves information search that is necessary for closing an immediate knowledge gap. Once that gap is filled, individuals might not continue to be curious. On the other hand, interest describes a knowledge seeking process that focuses on a particular content. Triggers for curiosity are based on uncertainty, complexity and novelty, which are different from the factors triggering interest. Curiosity lasts for as long as the knowledge gap remains to be filled, whereas interest might continue and grow along the interest development continuum. Hidi and Renninger concluded that more research is needed to further clarify the implications of curiosity and interest for educational practice and how curiosity could be used to trigger and promote the development of interest. Against the backdrop of this debate, I side with Renninger and Hidi in distinguishing curiosity from interest and argue that curiosity in cyber security seemed to proceed the development of related situational interest. More research would be beneficial to highlight how curiosity can better serve the development of cyber security interest, especially given that CCIT participants claimed it was their major “trigger.” In particular, it would be worth exploring through which content and in what context CCIT participants became curious about cyber security. Findings in this research highlighted that this could occur quite randomly, for example, when students saw the news about significant cyber security incidents or when they were scrolling through social media. Further research could be beneficial to understand when, how, and what type of cyber security content could spark curiosity in students, hoping they would then develop a more robust cyber security interest.

Perhaps the most relevant finding on triggers and interest development was CCIT’s role. Before receiving information on the CCIT, many students admitted that they were not familiar with the cyber security world. They declared that, without the CCIT, the topic would have remained unbeknownst to them (section 5.2.3). This is an important finding because it adds a welcomed dimension to the CCIT as an “interest generator” and not only an “interest influencer.” This thesis found that the CCIT seemed able to positively influence the cyber security interest of

participants. However, there was less expectation that it would trigger it in the first place, mainly because of the high knowledge barriers that a national-level event such as the CCIT could demand in order to attract highly talented individuals. In fact, the scientific literature seems silent on the possibility of programs such as skills competitions to trigger situational interest, although Renninger, Bachrach and Hidi (2019) found that overcoming a challenge, the use of computers and "fancy" technology, group work and hands-on activity, which are all ingredients of the CCIT, could elicit situational interest. In this regard, one element that might explain why the CCIT acted as a trigger was the admission process. Indeed, the admission process requested expertise in logic and programming, which are knowledge and skills that are more widely available than cyber security knowledge and skills. By using admission criteria that were more generic and in possession by a wider audience, the CCIT caught the attention of and recruited those who could have been intimidated by a cyber security skills competition with the goal of selecting young cyber security specialists right from the start. It follows that if NCSSCs aspire to be interest generators, they ought to maintain a more generic admission process.

On a very practical level, this sheds a different light on one of the major "success factors" of a competition as claimed by national organizers in an ENISA report (De Zan & Yamin, 2021), namely its public relations and marketing strategy. The report found that such a strategy had multiple purposes, including "at the beginning (…) raising interest among students." Nonetheless, this claim had never been validated by solid evidence. As a NCSSC can act as a trigger of cyber security interest, this research advanced that its ability "to be noticed" by the widest audience possible through a well-articulated and targeted public relations and marketing campaign becomes central. In the case of the CCIT, 70% of individuals became aware of the competition through their high schools and university departments, which underlines the importance of involving secondary and higher education institutions in the recruitment process. Comparatively speaking, the CCIT is one of the

competitions that does a better job at recruiting students in Europe,[49] even though its numbers are still small compared to the UK's Cyber Discovery programme, which was able to involve approximately 29,000 students on a yearly average in its first four years of infancy (Campbell-Jack et al., 2021a). If a NCSCC is a trigger of cyber security interest, NCSSCs could look at the UK case study to make their events even more wide-reaching.

9.1.2 The relationship between interest development and vocational interest

The second contribution of this thesis to interest theory is related to the differentiation that CCIT participants made between interest in cyber security as a topic and as a career. This is an essential contribution because, as the literature noted, vocational interest is not typically referenced in motivation research, and coordination between research on interest development and vocational interest could be beneficial (K. Ann Renninger & Hidi, 2011). To summarize, this thesis found that CCIT participants were more interested in cyber security as a topic than in cyber security as a career (section 7.2). As further evidence, participants had difficulties laying down concrete educational and professional future plans. Results revealed that participants were less inclined towards a cyber security career mainly because they did not want to commit to a specific path, lacked awareness about the cyber security sector and had "competing interests" (section 7.3). These findings have two implications.

The first one is related to cyber security competitions and the need for those in charge to avoid assuming that raising interest in cyber security as a topic means that interest in cyber security as a career will also be raised automatically. In other words, raising interest in cyber security as a topic and as a career are two different objectives and therefore need different sets of means to be reached. I will discuss

[49] Measured in terms of signups: According to an ENISA report, the CCIT has the highest number of subscriptions (4.452) among NCSSCs in Europe after the Czech Republic (over 5.000) (De Zan & Yamin, 2021).

this in section 9.3 when analyzing the findings on the relationship between skills competitions and the concept of interest.

The second implication is related to interest theory. Results suggest that a useful line of research could be to further unpack the association between interest development and vocational interest. The findings indicate that not all subject-interests lead to vocational interest. In fact, students' interest in cyber security did not mean they were equally interested in becoming a cyber security professional. Interviews suggested that vocational interest implied something more substantial, a deeper relationship with the subject the interviewee was interested in. To use interest research vocabulary, I did not expect students with a situational interest in cyber security to be interested in the profession as well. However, I expected this to be the case for those showing either an *emerging individual* or a *well-developed individual interest*. Although this would need further theoretical refinement and empirical analysis, one could theorize that vocational interest may sit right after a well-developed individual interest on Hidi and Renninger's interest development continuum. In other words, before becoming interested in a career, an individual must display a well-developed individual interest in a specific topic (figure 41).

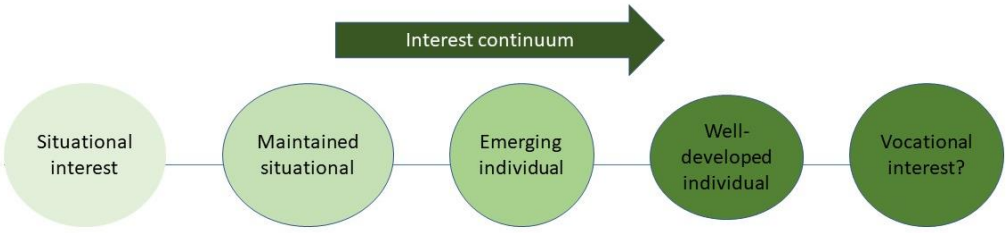

FIGURE 41 INTEREST CONTINUUM WITH VOCATIONAL INTEREST

In pursuing this line of research, it would be essential to formalize what characteristics or actions a learner would exhibit and undertake when vocational interest emerges. In the context of this research, interviewees with a cyber security career interest were more likely to have clearer intentions about their educational

and professional paths, were able to mention a specific cyber security task or profession they were more attracted to, and had no other particular competing interests. I believe understanding the relationship between interest development and vocational interest is very relevant in the context of interest research as, at the moment, there is a clear gap. Stakeholders expect programs such as skills competitions to increase both interest in a topic and a career, but if the relationship between these two distinct variables is not well-understood, these programs may not generate the expected outcomes.

9.2 A cyber security interest development system

Findings on the triggers and development of cyber security interest are essential to provide further specificity to interest research, but they are also important in helping explore the cyber security skills shortage (CSSS) more holistically. The purpose of investigating the origins of cyber security interest was to obtain the most comprehensive overview of these factors, as it was recognized that generating interest "is a nuanced process that involves multiple triggers rather than a single trigger" (K. Ann Renninger et al., 2019, p. 8). Results on cyber security triggers made evident the need to create a system to deal with the shortfall of security professionals more holistically.

The first part of this section argues that a first concrete step to create a solid pipeline of cyber security graduates would be the formal inclusion of cyber security teaching into high school and university curriculums.

The second part argues that a NCSSC can become the cornerstone of a national cyber security development system if it manages to "meaningfully engage" most of the students it recruits.

The third part suggests that creating a sound cyber security interest development system targeting the supply of skills could fail unless demand (i.e. labour market and employers) changes how the cybersecurity workforce is recruited and managed.

The fourth and final part evaluates NCSSCs as one element of a broader policy system aimed at creating a sustained national cyber security workforce. This section discusses the critical question of how effective skills competitions can be relative to other policy tools.

9.2.1 Building the foundation of a cyber security workforce: the inclusion of cyber security formal education curriculums

This research recognized that, especially when the units of analysis are NCSSC participants, interest in cyber security does not just happen, and it usually represents the culmination of many years of interest development in computer science. In fact, 80% of individuals who signed up to the CCIT were studying or had studied computer science and programming, which replicates findings from Cyber Discovery, where 81% had studied computer science at some level (Campbell-Jack et al., 2021a). Therefore, a cyber security skills strategy aimed at creating a sustained national pipeline of cyber security professionals must first ensure there are enough incentives motivating students to pick up a passion for IT technology. This research found that six main factors contributed to the development of participants' interest in technology and computer science, namely:

- Gaming
- School activities involving IT tools
- Desire to understand how a computer works
- Parental support to pursue computer science
- Programming and experimentation
- Self-learning

More than providing an encompassing list of computer science triggers, which was not the focus of this research, these findings provide background and underline that, at least for NCSSCs' attendees, cyber security interest is likely to have grown from a more general interest in technology. However, this research contribution is

content-specificity, and therefore its ability to have identified the triggers that are peculiar to cyber security (section 5.2), which were:

1. Curiosity
2. Coursework
3. The CCIT
4. Encouragement coming from an educator
5. TV shows
6. Reading technical documentation
7. Cyber security skills competitions
8. Friends and family

By looking at this list, it is clear there exist several access points to cyber security and several triggers that can promote an inflow into the sector. It would be harder to turn all these triggers into policies scalable at the national level, which is what a country-level issue such as the CSSS requires. Hence, if one had to choose the triggers to use in order to design cyber security interest interventions, policymakers should probably start with what policy could more easily implement and shape: the formal inclusion of cyber security into secondary and higher education curriculums and the organization of a national cyber security competition.

Despite issues in the provision of computer science education in formal settings (section 5.1.4.2), the inclusion of cyber security into high school and university curriculums could have the most important impact because of its potential nationwide reach. In the Italian secondary education system, cyber security education would have to be levelled according to the type of high school. It would probably make little sense to teach advanced cyber security knowledge and skills in high schools focusing on humanities and social sciences such as the “classics” or the “linguistics” lyceums. However, it seems surprising that, in 2021, cyber security has not been fully included in the computer science curriculums of the “applied sciences” scientific lyceum or the “computer science and telecommunications” technical institute, the schools of provenience of most CCIT participants.

Clearly, the content and delivery of cyber security teaching would need to be tailored. For example, in the context of humanities and social science lyceums, cyber security could be included in a broader curriculum on computer literacy, where students would learn about cyber threats and how to protect themselves. Meanwhile, in STEM-focused institutions, deeper cyber security concepts and techniques should be included in computer science education, if not studied on their own. If policymakers decide to add cyber security education into the secondary education curriculum, finding enough qualified staff to teach security knowledge and skills could be an issue (Pencheva, Hallett, & Rashid, 2020). While this is certainly a problem, one could also wonder whether some serious investments in cyber security education, which is often allocated less budget compared to other cyber security policy areas, could help alleviate this issue.

At the university level, many have urged including cyber security education in computer science teaching. For example, Krutz and Richards (2017) found that only one out of the 36 highest rated computer science degrees in the United States required cybersecurity coursework. As students who show a basic understanding of cyber security usually have a competitive advantage when they apply for jobs, they suggested universities need to teach more cyber security. Even this research found that the lack of cyber security education is an obstacle in creating a cyber security workforce, with interviewees lamenting the lack of courses/degrees and high entry requirements (section 6.2.3). The fact that the mere availability of relevant degrees could be an essential factor in a cyber security interest development system was demonstrated by this research as well. Indeed, one student, who had not been admitted to the CCIT, said that her interest had increased because her university had recently opened a new cyber security master's degree, giving her another chance to get involved in cyber security. To avoid the risk of turning students into different educational paths, the provision of cyber security education should be aware of all the issues that are currently affecting its delivery at the university level (W. A. Conklin et al., 2014; Crumpler &

Lewis, 2019; Gagliardi et al., 2016; Schneider, 2013) and remediate them to the best extent possible. Nonetheless, at this point, given the urgent need for well-prepared cyber security students entering the labour market, the systematic inclusion of cyber security education into university teaching would likely do more good than harm.

The bottom line is that adding cyber security to curricula would be a first very concrete step to make students aware and knowledgeable (at different levels) about the subject, and from then on, start building interest among those who show a predilection for the topic.

9.2.2 NCSSCs as the cornerstone of a national cyber security interest development system

As evidenced by the findings of this research, the establishment of a national cyber security competition like the CCIT is another concrete step that decision-makers could take to build an effective cyber security interest development system. The prior section has already pointed out the role of the CCIT as an interest trigger; the next section will analyse the extent to which and how the Italian skills competition seemed to have increased interest in its participants.

As the purpose of this section is to place cyber security interest triggers within a broader policy system, I posit that a NCSSC could have an even more significant impact if it succeeded in “meaningfully engaging” most of the students it recruits. The example of the CCIT is illustrative. Approximately 4,450 students signed up to the CCIT, but only 560 were admitted to the competition. Because of Covid-19, CCIT organizers implemented the OCCIT programme, a spin-off of the actual CCIT competition, which allowed students who had sat the admission test to access some learning material and on-demand skills challenges. According to organisers data, of the 511 students who enrolled in the OCCIT, only 28 completed it. Therefore, the CCIT meaningfully engaged “only” 588 participants (560+28) out of 4,450, meaning 13% of all students who had been recruited and who had shown

interest in the programme. This is in line with what was found by an ENISA report, which showed that only 11% of the students recruited by NCSSCs in Europe were “active” users (De Zan & Yamin, 2021). As a reference, UK Cyber Discovery recruited 35,941 students in the 2019/20 edition: 33,427 went through the first assessment phase, and 10,564 (29%) accessed the following phase called “Game,” which consists of hundreds of hours of gamified challenges in various cyber security domains (Campbell-Jack et al., 2021a), and thus can be considered a training. This attrition rate is probably due to the fact that NCSSCs also have the goal “to identify talent,” an elite group of students who are selected to form the national team and attend international cyber security competitions (such as the European Cyber Security Challenge). However, in the context of a cyber security skills shortage, national skills competitions should aim to meaningfully engage the highest number of people they recruit, especially given the likely efforts and resources they put in their marketing and public affairs strategies. If the cyber security shortage is a quantitative issue (i.e. the number of students entering the sector), it is probably more important to increase the interest of the largest number of students possible rather than nurturing a small group of elite students. As well-developed NCSSCs like the CCIT or Cyber Discovery already possess such technology, a solution could be to give access to most students to their online platforms and engage them through a mix of online training and skills challenges, and perhaps additional triggers such as cyber security news, technical documentation, videoclips from pertinent cyber security TV shows and guides to educational opportunities and careers.

To conclude, in the context of the CSSS, NCSSCs should be more focused on meaningfully engaging the highest number of students rather than selecting small elite groups of students. Moreover, they should also exploit the scalable solutions offered by their online platforms. This could make NCSSCs the cornerstone of any national cyber security interest development system.

Once cyber security education is further embedded in the education system, and a NCSSC is established, relevant stakeholders can be creative and include more triggers and factors within already established policies. For example, it could be hard to establish a programme telling parents to encourage their children to join the ranks of cyber security workers. However, in the context of a taught cyber security course, educators can think of running informative workshops for parents to inform them about the educational and professional opportunities that cyber security offers, hoping that parents will then help their children make informed choices. In addition, during a cyber security class at university, professors might explain a concept with an example taken from news coverage, eliciting students' curiosity, who could see the real-world application of what they study. By way of another alternative, as many interviewees were attracted by role models such as the main character in *Mr. Robot*, videoclips from such TV shows could arouse the interest of students who had not been previously exposed to cyber security.

In sum, the cyber security triggers found in this research are not all suitable to be turned into a national policy with the expected impact of increasing cyber security professionals. Nevertheless, they are cyber security-specific and likely to work in several contexts. Hence, they should be taken into account by decision-makers at all levels (policymakers, educators, programme designers and implementers, etc.) to create a holistic strategy to address the cyber security skills shortage.

9.2.3 The labour market's role in mitigating the skills shortage

The problem is that creating a sophisticated cyber security interest development system will be of no use if the labour market is unable or unwilling to solve the issues currently affecting demand. In other words, investing public resources to make sure that well-prepared cyber security students are ready to enter the cyber security sector is of little help if employers do not change their requirements and better manage their cyber security workforce. There is now ample evidence that

demand is creating labour market bottlenecks that impede the proper allocation of the cyber security skills supply. The most significant issues are:

- *Unrealistic job requirements*: currently, companies are often looking for mid-level cyber security professionals with at least five years of relevant experience and possessing relevant degrees and professional certifications (Burningglass, 2019; ISACA, 2020; McHenry et al., 2021; Oltsik, 2021). One paradox that is often mentioned occurs when businesses look for junior professionals with the Certified Information Systems Security Professional,[50] an industry certification that people can attempt to obtain only after having gained five years of professional experience;
- *Lack of cyber security training*: employers rarely offer the correct cyber security training to their employees, or there is rarely time to invest in upgrading skills (ISACA, 2020). In a recent study, 59% of cyber security professionals agreed that job requirements often impede adequate skills development (Oltsik, 2021);
- *Lower-level salaries compared to what a cyber security professional can command*: cyber security professionals often think that the lack of competitive compensation is "the biggest reason the cyber security skills shortage is impacting their organizations" (Oltsik, 2021, p. 4);
- *Human resource departments struggling to understand and communicate cyber security jobs requirements*: HR managers do not adequately understand cyber security roles and tasks with the consequence that they write conflicting and unrealistic job descriptions and skill requirements for their vacancies (ISACA, 2020; McHenry et al., 2021; Oltsik, 2021).

While this research was not concerned to identify challenges on the demand side, it also found similar evidence. For example, sections 6.2.3 and 8.3.3 showed a student's frustration regarding employers' claims about the alleged need of cyber

[50] CISSP is an independent information security certification granted by the International Information System Security Certification Consortium. It is one of the most coveted industry certifications in the cyber security labour market (Oltsik, 2021).

security professionals vis-à-vis the scarce availability of entry-level opportunities in the sector.

Hence, because skills issues could be generated on both sides of the labour market, some scholars suggest that governments should move away from policy programs targeting the supply side and instead focus on demand's issues (Buchanan et al., 2017; Mayhew & Keep, 2014). A solution could be to "branch out and to adopt policies that see education and training as a component within a much broader set of policies concerned with economic development, business improvement, workplace innovation, productivity growth, and job quality" (Keep, 2017, p. 2). Given the complexity of the CSSS, and the issues that are affecting supply as much as demand, I would contend that governments should have an active role in helping companies to have a wider pool of qualified candidates from which to recruit junior professionals, which is indeed what is happening in policy-savvy countries such as Australia and the UK (Australian Government, 2020; HM Government, 2018a). Nonetheless, employers should also understand their role in creating a more consistent supply of cyber security skills and remove those barriers that create unwanted obstacles in creating a national cyber security workforce.

In the end, the main takeaway from this section is that asking a NCSSC (or any other single policy) to solve the CSSS on its own would mean failing to understand the complexity of the problem and over-estimating what an out-of-school time activity like a skills competition can achieve. A NCSSC can neither be a substitute for a modern education system that is somehow reflective of labour market demands nor a panacea for employers with unrealistic expectations about the cyber security workforce. A NCSSC should be one of the elements in a broader policy system that clearly understands the challenges posed by the CSSS and has the resources and persistence to cope with it.

9.2.4 Skills competitions and the concert of cyber skills policies

This thesis found that the CCIT reached its intended objective of increasing participants' cyber security interest. Moreover, it was, unexpectedly, among the factors contributing to forming cyber security interest in the first place. For these reasons, it should be considered an "effective" policy to mitigate the cyber security skills shortage as it tackles one of the issues currently compounding it, namely the low interest of young people in pursuing cyber security.

However, NCCSCs are tasked to solve only one of the issues that are currently worsening the CSSS. In fact, there are at least four main problems that are affecting cyber security supply and demand: 1) the education system's inability to equip students with the "right" knowledge and skills; 2) the low number of students interested in cyber security coming out of the education pipeline; 3) employers providing few entry-level opportunities; 4) employers investing little in their cyber security workforce (i.e. offering lower-level wages and limited training opportunities) (Bate, 2018; De Zan, 2019a).

Looking at the CSSS more holistically, it is clear that such an issue can only be confronted with a system of policies addressing the various facets of the problem. For example, if a government needs more graduate students coming out of the education pipeline, it might correctly sponsor the establishment of more cyber security master's degrees. However, bachelor's students might not be interested in enrolling. If this occurs, a government would be forced to implement at least two policies to succeed: one pushing bachelor's students to join cyber security master's degrees and another intervention setting up these degrees. This is if the government looked at the CSSS as a skills supply issue only.

However, as seen above, the CSSS is deteriorated by issues located on the demand side as well. Hence, if policymakers do not look at the problem holistically, they may soon realize one paradox: even after having targeted the education and training system with successful interventions and having created a supply of qualified cyber security graduates, the CSSS will not be mitigated if the labour market does not absorb them by offering entry-level opportunities.

Because the CSSS comprises all these issues at the intersection between supply and demand, this chapter argues in favour of a policy system rather than a single intervention approach. Looking back at the literature on cyber security skills shortage policies, authors have proposed various tools (see section 2.2.2 for a thorough discussion). The figure below helps visualize how a NCCSC would "fit" into a cyber security skills shortage system.

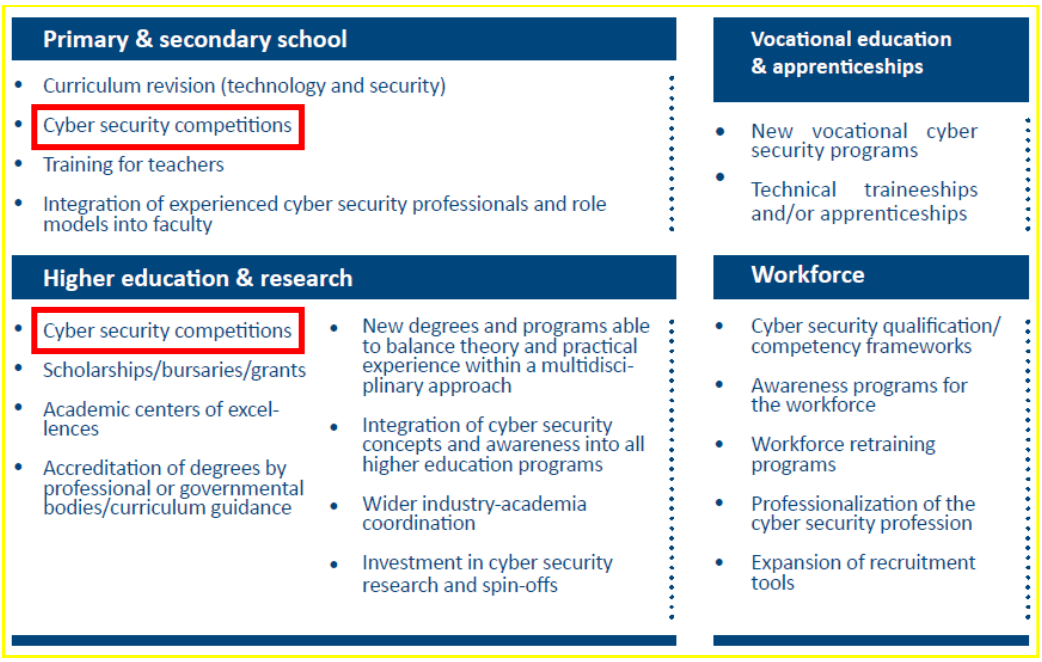

FIGURE 42 OVERVIEW OF CYBER SECURITY EDUCATION AND SKILLS POLICIES OF SELECTED COUNTRIES. SOURCE (DE ZAN, 2019A)

It is difficult to compare NCSSCs with other cyber skills policies, mainly because their nature, structure, implementation and objectives are different. However, it is useful to consider NCSSCs in this broader context for a discussion on how these policies relate to one another.

For instance, section 9.2.1 posited that compulsory cyber security teaching may have a wide impact because of its potential national reach. Using the Italian context and the CCIT as an example makes this clearer. The CCIT recruited 4,454

students, and 71% of participants in the second survey (N= 390) stated that the CCIT had increased their interest in cyber security as a topic. At the population level, this means that the CCIT might have increased interest in 3,162 students. According to data from the first survey, the CCIT attracted mainly high school students enrolled in scientific lyceums ("applied sciences" curriculum), high school students enrolled in technical institutes ("computer science and telecommunications" curriculum) and university students enrolled in computer science degrees. Unfortunately, there are no specific data on the number of students enrolled in the "computer science and telecommunications" curriculum or computer science degrees. However, we know the exact number of students enrolled in applied sciences – scientific lyceums in the 2021/22 academic year, namely 210,220 (Ministero dell'Istruzione, 2021a). If policymakers had decided to introduce a cyber security course similar to CCIT training in these schools, and assuming (conservatively) that at least 25% of these students had increased their interest in cyber security as a topic, the intervention would have augmented cyber security interest in 52,555 students. Less conservatively, and assuming that at least 40% of them had increased their interest, cyber security teaching could have affected 84,088 students vis-à-vis 3,162 affected by the CCIT. Note that this estimate considers introducing a cyber security curriculum to applied sciences – scientific lyceums only. Hence, this estimate is likely to be far greater if a cyber security course was introduced in technical institutes or computer science degrees, the other "recruiting grounds" of the CCIT. Introducing compulsory cyber security teaching at selected secondary and higher education institutions would not come without challenges, including curriculum design (Blair, Hall, & Sobiesk, 2021; Dan, Kohnke, & Sigler, 2021), finding enough qualified teachers and lecturers (Pencheva et al., 2020), and more generally finding the financial resources to teach a complex subject to a large number of students nationally. Nonetheless, if governments were serious about tackling the shortage, they would put serious thought into providing introductory cyber security courses to their students.

A different way to gauge how a NCSSC is related to other cyber security skills policies is to compare its outcomes with those of other policies, although one

should be fully aware that different interventions are likely to be different in nature and have different goals. The literature review warned that, like for generic skills shortage policies, there is little evidence of what has been working to mitigate the lack of cyber security experts because governments have generally not put in place serious evaluations mechanisms (CEDEFOP, 2015; De Zan, 2019a; Garcia-van Hoogstraten & Bate, 2019; The Secretary of Commerce and the Secretary of Homeland Security, 2017). One valuable exception is the UK, whose government has evaluated the cyber skills policies implemented in the last years. Recently, it has published a series of reports helping us put in perspective the concert of policies required to tackle the shortage. Below, I summarize the main elements of these evaluations:

- **Cyber Discovery**: It was a government-funded extra-curricular skills competition for secondary students aged 13-18 aimed at ensuring that as many students as possible enter the cyber security profession. It was launched in 2017 and engaged on average almost 29,000 students per year until it was discontinued in 2021. The evaluation stated that the programme increased computer science and cyber security skills, but found no evidence it increased interest in cyber security as a topic or as a career (Campbell-Jack et al., 2021a).
- **CyberFirst**: The overall objective of CyberFirst was to create a pipeline of cyber security talent to supply the UK labour market. The programme was made up of several interventions. The evaluation focused on CyberFirst summer courses, which involved 1,627 participants, and found that: cyber security interest did not increase (it remained high); students stated their knowledge and skills had increased; they were more likely to consider applying for a cyber security degree, bursary and apprenticeship and consider a cyber security career (Campbell-Jack, Bickley, & Lillis, 2021b).
- **Cyber Security Postgraduate Bursaries Scheme**: The goal of the intervention was steering graduates toward cyber security through accredited MSc programmes. A total of 118 bursaries were awarded. Although the evaluation could not report on actual career choices (most

students had not graduated yet) limited evidence suggested that the scheme was making students transition into the sector: three-quarters of them thought that completing the course was going to help them get a cyber security job (RSM, 2020c).

- **Cyber critical national infrastructure apprenticeships programme**: The programme aimed to encourage the uptake of apprenticeships in the wider economy and specifically within critical national infrastructures. The report considered apprenticeships on the level 4 cyber security technologist standard over the period 2017 – 2019, in total 51 apprentices (the original target was 150). The evaluation found that companies were content with the progress made by their apprentices in terms of cyber security skills, the ability to identify risks and think more about cyber security issues relative to their business (RSM, 2020b).
- **Cyber Skills Immediate Impact Fund**: the policy sought to train individuals not currently employed in the cyber security industry for entry-level opportunities in the sector, while boosting diversity. The evaluation analysed that 480 individuals took part in the training initiative, and while almost 75% of them were still completing it, the intervention increased cyber security knowledge and skills (over two-thirds of respondents) and employment outcomes (35.7%) (RSM, 2020d).

To conclude, this section placed a NCSSC within the broader context of policies that can be implemented to increase cyber security interest and mitigate the cyber security skills shortage. Following up on section 9.2.1, it showed that, in the Italian context, compulsory cyber security teaching in secondary and tertiary education could potentially have a much bigger impact than the CCIT because of the national character of the policy. However, this assessment remains “theoretical” as adding cyber security teaching would present challenges such as curriculum design, finding enough educators, providing the right infrastructures and resources. This section also showed how Cyber Discovery, the UK NCSSC, could be related to

other policies that have been used by HM government to increase the cyber security pipeline. It presented evidence that, while Cyber Discovery reached a much higher number of students compared to other programmes, the intervention was apparently unable to deliver the intended outcome (even though the evaluation report acknowledged some serious methodological issues in the analysis).

The main takeaway of this section is that the impact of a NCSSC will also be contingent upon the national system in which it is implemented. In Italy, compulsory cyber security teaching in technical schools and universities would likely have a larger impact than the CCIT. Nonetheless, the reality is that changes to curriculums are unlikely to happen soon, which means that the CCIT will remain among the best chances for Italian students to become interested and knowledgeable about cyber security for the time being. In a more articulated policy context such as the UK one, instead, policymakers need to evaluate which policies (after comparing them and performing cost-benefit analyses) are more suitable to reach the intended national objectives. Hence, in these countries, a NCSSC might not be the best policy solution to reduce the skills shortage.

9.3 The influence of a national cyber security skills competition on interest

The research contribution made by this thesis does not end with interest theory. The literature review found that skills shortage policies have been under-researched and, as NCSSCs have been used to mitigate the lack of security professionals, more work is needed to deal with labour market and skills issues effectively. The literature also highlighted that educationalists had had ambiguous attitudes towards skills competitions as there is no agreement on the pros and cons of incorporating them in educational settings. Moreover, there is also a niche literature on the relationship between skills competitions and participants' interest, whose results on competitions' outcomes have been mixed. Finally, as NCSSCs

are now the most implemented policy to counteract the shortage, having a better understanding of their results is essential to inform governments that are trying to maximize their outcomes. By analysing the extent to which and how the CCIT influenced cyber security interest among its attendees, this section reflects upon this research's contribution to these interconnected strands of social science literature and policy debates.

Although there are limitations to this thesis' causation claims (see section 10.2), the first part of this section contends that the CCIT positively influenced participants because of the way it recruited and the three-month cyber security training. It also urges all NCSSCs, in Europe and beyond, to include cyber security training to have a more profound impact on the skill shortage.

The second part of this section maintains that the CCIT still increased interest in a cyber security career, but less compared to interest in cyber security as a topic. The CCIT was slightly less effective because vocational interest in cyber security was lower before the beginning of the CCIT, less emphasis was put on career awareness by the CCIT, and the timing of the intervention was not ideal for many participants. These findings have several implications, the most important one being the need to refocus attention on implementing well-designed career awareness activities, when resources allow it.

9.3.1 The influence on cyber security as a topic

This thesis suggests that a NCSSC such as the CCIT could have a "positive" influence on participants, as 71% of attendees reported that the CCIT had increased their interest in cyber security as a topic. It can be claimed that the CCIT did have an "effect" as the students who underwent the programme said their interest had grown more than students who were not admitted. However, an important finding was that the CCIT increased interest in cyber security as a topic even among the students who did not access the training (section 7.1). Although there are limitations to the causation claims of the quantitative findings only (see

section 10.2), qualitative data added evidence and gave a greater understanding of processes and contexts. They revealed that if CCIT was the main factor increasing cyber security interest among TG participants, students in the CG also mentioned other elements. In other words, for CG students, the CCIT was a co-factor rather than the only reason their interest grew.

These are significant findings as they run against the initial hypotheses of this research, which posited that the CCIT would have induced an overall decrease in cyber security interest in the population. More specifically, the CCIT would have kept interest levels equal in TG participants and decreased interest in the CG. The logic was that interest in TG participants would have remained the same because attending the CCIT would not have been a game-changer for them. As these students had developed strong interest and skills before entering the competition, undergoing a skills programme based on topics they had already been exposed to was unlikely to change how they felt about cyber security. On the other hand, cyber security interest in CG participants should have decreased because students could have been upset about failing the admission test and the impossibility of exploring the cyber security sector further through the training programme. Their failure could have made them think that their skills were not good enough compared to those of their more gifted peers. This could have persuaded them to give up on cyber security. The findings did not confirm these hypotheses mainly for two reasons linked to the admission process.

The first reason is that the students who did not pass the admission test were not upset or demotivated to the extent that they ultimately gave up on cyber security. Most of the interviews confirmed CG students were disappointed at the outcome of the admission process, but most importantly, the disappointment did not lead to any “abandonment” of cyber security. CG participants considered the test both appropriate and challenging but also fair in selecting the suitable candidates to undertake the CCIT. Moreover, for some, the CCIT admission still acted as a catalyst, putting cyber security on their radars; for others, the failed attempt was a moment of reckoning that encouraged them to achieve better results. Overall, CG

participants showed determination and grit rather than disillusionment and negative feelings towards cyber security. What emerged strongly was their willingness to learn from their mistakes and progress in their cyber security skills development journey.

The second reason is that the admission test did not select those students the hypothesis foresaw the CCIT would recruit. The CCIT admission process did not select young cyber security specialists but instead attracted mainly computer science “generalists” with high-level logic and programming skills. While most TG participants clearly had an interest in cyber security before starting the CCIT, most of them did not have much first-hand exposure. Because of that, the programme had room for manoeuvre in influencing their interest. Clearly, had the CCIT been an unsatisfactory experience, participants’ interest would have likely diminished. However, because the CCIT was successful and selected computer science generalists rather than cyber security specialists, it influenced their interest to a greater extent than the initial hypothesis thought was achievable.

One of this thesis’s most important contributions is explaining and describing how the CCIT achieved to influence participants’ cyber security interest (ch. 8), an explanation which is helpful for both practice and theory.

The most important finding was that cyber security interest was mainly influenced by the three-month cyber security training (section 8.3.1). Students particularly enjoyed receiving cyber security foundational knowledge and the practical, hands-on lab exercise. In this context, they were favourably impressed by their instructors’ expertise, as well as their willingness to help. The importance of training had been highlighted before in the literature, but it had been seen as an instrument to lower entry-level barriers (Cheung et al., 2012; Werther et al., 2011) and improve students cyber security knowledge and skills (A. Conklin, 2005; Leune & Petrilli, 2017; L. McDaniel et al., 2016; Mullins et al., 2007), but not to raise cyber security interest. This finding has two implications.

First, it is telling that in the context of a programme that is publicized as a skills competition, whose skills challenges represent the culmination of the whole event, the factor that raised students' cyber security interest was the training rather than its competitive component. Choosing to integrate a relatively long and well-structured training programme within an NCSSC like the CCIT made sense because of the profile of candidates and the overall policy context. As the CCIT mainly targeted computer science generalists, it would have made little sense to rush them into a competition they were unprepared for. As much as these students clearly loved the thrill of a skills challenge, interviews revealed how meticulous and systematic they were in acquiring knowledge in the topics they were interested in before attempting to compete. Participants vastly preferred the June local challenge to the October national one as they felt the training had prepared them well to tackle the former, but not the latter. In sum, these findings suggest that an NSSSC better achieves its goals when skills challenges are preceded by training and the competition is not the only component of the programme or an end in itself. Furthermore, a NCSSC designed around training and skills challenges more coherently fits the current policy setting. If the goal of NCSSCs is to equip more students with the proper cyber security knowledge and skills to enter the labour market, it is sensible to target computer science generalists (with low-to-medium prior exposure to cyber security) and put them through a programme designed to raise their interest, rather than recruiting a minority of already gifted students and make them compete in a one-day skills challenge.

The second implication is that these findings made the obvious case for the systematic inclusion of cyber security training within NCSSCs. This is not a trivial suggestion as currently, there seems to be little awareness, or perhaps a lack of resources, to fully incorporate cyber security training in national skills competitions. An ENISA report found significant variance in cyber security training within competitions across Europe, with many differences in the type, duration, and target group. For example, if Italy trains 560 individuals for three months on one side, on the other side, there are countries like France training only ten individuals for less than a week (figure 42) (De Zan & Yamin, 2021). In the light of the research results,

the inclusion of cyber security training in NCSSCs seems even more warranted as competitions generally aim to raise cyber security interest among participants, but many do not resort to the main ingredient (i.e. cyber security training), to achieve that.

FIGURE 43 NUMBER OF TRAINEES AND DURATION OF TRAINING IN NCSSCS ACROSS THE EU. SOURCE: DE ZAN & YAMIN, 2021)

9.3.2 The influence on cyber security as a career interest

The findings on the influence of the CCIT on cyber security career interest deserve a separate discussion because the literature has highlighted the need to further study the relationship between interest development and vocational interest (K. Ann Renninger & Hidi, 2011) and because our understanding of how skills competitions can influence career interest is limited, yet very relevant in the context of a skills shortage.

To summarize the findings, students stated in the post-survey that the CCIT had indeed increased their interest in a cyber security career. Similarly to the results

on interest in cyber security as a topic, the CCIT seemed to have exerted an influence as TG attendees declared their interest grew more on average in comparison to CG participants. Nonetheless, the CCIT had a more significant effect on participants' interest in cyber security as a topic than as a career: 71% of attendees declared that the CCIT had either significantly increased or increased their cyber security topic interest, compared to 49% who stated the same about interest in a cyber security career (section 7.2). One can attempt to give three explanations for this result.

First, students were more interested in cyber security as a topic than as a career before the start of the competition, and the CCIT was unable to change that. Unwillingness to commit, uncertainty regarding the future and other competing interests were all plausible explanations justifying this lower interest in a cyber security career (section 7.2.2.2).

Second, from the account provided by the interviewees, the CCIT perhaps put less emphasis on career awareness activities than on training. In fact, it seemed that the organization of career awareness activities had been delegated to the individual universities, with students reporting very different experiences. Moreover, the seminars organized with the sponsors of the competition received mixed reviews, with attendees being seemingly indifferent or even critical with respect to the content of these meetings. These findings seem in line with an ENISA report, which found that efforts to develop links with employers could be improved. The report talked expressively about an "under commitment" of EU NCSSCs to cyber security careers (De Zan & Yamin, 2021), which is at odds with their expected impact to help to deal with the shortage of cyber security professionals.

Third, it seems that the timing of the CCIT was not ideal to influence most students' career interest, and this had to do with the age group the CCIT recruited from. The CCIT allowed students aged between 16-23 years to access the admission test. However, the latest Almalaurea report on the profile of 2020 university graduates in Italy found that students enrolled in computer science-engineering bachelor's

degrees usually graduate when they are on average 23.8 years old; they are on overage 26.5 years old when they graduate from a master's degree (Timoteo et al., 2021). This is perhaps why CCIT participants were more focused on continuing or finishing their studies than looking for a job. This timing issue came up clearly during interviews, for example, when a couple of students from the TG, whom companies had contacted for placement opportunities, declined their offers stating they preferred to conclude their studies.

One implication of this finding is that the relationship between interest development and vocational interest should be further explored, as suggested in section 9.1. There are, however, four other implications that are relevant for NCSSCs' designers.

The first is that it cannot be assumed that when a NCSSC influences interest in cyber security as a topic it influences cyber security career interest to the same extent. This is also what was suggested by Campbell-Jack et al. in their review of Cyber Discovery:

> "Therefore, the extent to which Cyber Discovery changes career consideration is a crucial question for future programme development. Information in this report suggests it should not be automatically assumed that taking part leads to improved career consideration although it may be that increased knowledge leads to a better alignment of career options among participants, including some understanding it is less of an option for them (2021a, p. 68)."

This suggests that different tools should be thought about and developed to increase career interest. In other words, cyber security training cannot be assumed to also raise career interest, and other career awareness activities must be designed to make participants think more actively about cyber security careers.

The second implication is that more effort, rather than less, should be put into designing cyber security career interventions. This would require a paradigm shift as currently more emphasis is put on implementing training activities and skills challenges, which is somewhat natural as NCSSCs' organizers are often computer science educators and not career awareness and guidance professionals. More

efforts towards this endeavour are necessary for two reasons. First, at least in the context of the CCIT (but also Cyber Discovery, see Campbell-Jack et al. (2021a)), participants seem to start NCSSCs with lower interest in a cyber security career. Hence, if a NCSSC wants to offset this initial imbalance, it should double down on its career awareness activities. Second, this is necessary in the context of the CSSS. Most NCSSCs have been established to help mitigate the shortfall of cyber security professionals. Therefore, if NCSSCs genuinely wish to do so, stakeholders should realize that career awareness activities need the same amount of expertise, resources and time as cyber security training and challenges.

The third implication that stems directly from the first two is that NCSSCs designers need to develop more defined career awareness interventions throughout the programme. To the best of my knowledge, there are currently no studies exploring how career interventions can best be embedded in the context of NCSSCs. Although a good place to start would be the more general literature on career interventions (Hughes, Mann, Barnes, Baldauf, & Rachael, 2016; Pye Tait Consulting & Carol Stanfield Consulting, 2021; Whiston & Noblin James, 2012), specific research on career awareness activities organized within the context of NCSSCs is warranted as these activities would take place in contexts that are clearly different from purely educational settings. This research cannot pinpoint the exact career interventions that might be most effective as the influence of CCIT's career activities was hard to gauge. However, this study suggests that the timing and target group are essential factors to consider. While it is clear that the quality of any career interventions should be adequate, these may not produce any demonstrable outcome if they do not target the right participants at the right time. As suggested by the interviews, participants were not necessarily intrigued by career activities because, very simply put, they were not currently looking for employment. If one looks at the age group the CCIT recruits from (16-23 years) and the average age at which students start looking for jobs (23.8 years at the end of bachelor's or 26.5 years at the end of master's degrees), it is not completely unexpected that career awareness activities targeting de-facto high schoolers and students in the middle of their bachelor's degrees would have less of an influence

on students' cyber security career interest. There are no easy solutions to the issue of timing and target group. Organizers could decide to have different career interventions according to different age groups (high schoolers vs bachelor's students vs master's students) or have a NCSSC that recruits from an age group that is closer to when participants start seriously considering careers (for example, university students only). Either way, this will be contingent on the available resources and the objectives of the competition.

The fourth and final implication is that students who declare to be interested in a cyber security career might not, in the end, either choose to pursue or obtain a cyber security job. The following section will discuss that interest is different from career choice, which is affected by many other factors that cannot be manipulated by an NCSSC. Thus, stakeholders should be prepared to accept that not all of those entering a skills competition with an interest in a cyber security career will ultimately decide to join the cyber security workforce. This analysis mirrors what found by the researchers investigating the UK Cyber Discovery:

> "It is also important that 88% of Cyber Discovery participants stated at the Year Three post-survey that they were very or fairly interested in a career in cyber security, given the programme's objective to fill the existing cyber skills gap. However, it is unlikely that all of those who say they are very or fairly interested will progress into actually applying for relevant jobs, so this 88% figure will likely translate into much lower actual cyber career uptake" (Campbell-Jack et al., 2021a, p. 57).

However, other variables, analysed in the next section, can possibly better predict whether NCSSC participants will pursue a career in cyber security.

9.4 Is interest an adequate outcome by which to assess a national skills competition?

This final section is dedicated to analysing the relevance of the concept of interest when assessing skills competitions. It reflects on the adequacy of this concept as an outcome measure, going beyond it and considering other relevant variables,

which NCSSCs like the CCIT do not yet seem to include as their objectives. This research found that three outcome variables could be particularly indicative of the impact of a NCSSC on the skills shortage, namely educational and career planning, key education and career choices and competing interests.

The first part of this section posits that students' engagement in educational and career planning would be a useful outcome variable to assess NCSSCs, especially if more explicit links are established between the concepts of interest development and vocational interest. However, it warns that influencing career planning would be a complicated endeavour even for well-designed NCSSCs.

The second part argues that key education and career choices are an exceptional outcome measure to evaluate NCSSCs as they provide the hardest evidence of the effect of a programme in the context of a skills shortage. Similarly to planning, nonetheless, it may be difficult for competitions to influence key choices as they depend on factors that cannot be easily shaped by a NCSSC alone.

The third part claims that stakeholders should integrate competing interests in their analysis of NCSSCs if they wish to fully understand competitions' consequences and avoid falling into the "interest paradox."

Against this backdrop, however, the final section suggests keeping *interest* as an outcome of NCSSCs as it is the foundation stone of any encompassing and complete NCSSC assessment and a more achievable outcome than those above.

9.4.1. Educational and career planning

This study found that CCIT participants seemed to have little awareness of the cyber security sector both in terms of educational offers and professional roles: in the post-survey, 45% of participants declared to not know of any specific cyber security degree, while 55% stated the same about specific cyber security roles

(section 7.3).[51] Anecdotally, I recall sending to a couple of participants a weblink with a list of cyber security degrees at the end of our second interview, as they were lamenting that they did not know where to get information about such educational offerings in Italy. Regarding a career in the sector, interviews showed that the lack of awareness concerning cyber security as a profession often pushed students to avoid committing and assume a "wait and see" approach. Even when students showed a little more consciousness regarding their future intentions, they often cited the penetration tester as the cyber security role they aspired to, which is usually the first job that comes to mind because of the "hacker figure" dominating the image of cyber security (Shires, 2020), especially in the younger population. Rather than showing sectorial awareness, these students may have been showing a romanticized vision of a sector that has at least over 50 types of jobs in addition to the penetration tester (Newhouse, Keith, Scribner, & Witte, 2017). These results have two main implications.

The first implication regards the earlier debate on the relationship between interest development and vocational interest. This finding was somewhat surprising because, even though many participants displayed or talked about their vivid interest in cyber security, they often could not articulate ideas or plans on how they wished to take this interest forward. In a way, this appears to confirm that vocational interest emerges when interest is stronger, or, to use more appropriate interest research language, when this is either *emerging individual* or *well-developed individual*. Especially because it sits somewhere around the concepts of interest development and vocational interest, educational and career planning is well suited to be used as an outcome measure of NCSSCs. However, further research is needed to provide more explicit links on the interplay between interest development, vocational interest and educational and career planning. If it is found that the latter is closely related to vocational interest, and then perhaps career

[51] As a reference, this result seems in contrast with findings from the UK Cyber Discovery, where approximately 80% of participants declared that they had heard of cyber security degrees or apprenticeships (Campbell-Jack et al., 2021a).

choice, it could be a more robust indicator of the benefits of a NCSSC, given its aim to curb the shortage of professionals.

The second consideration regards the ability of a NCSSC to shape participants' career decision-making process. Results from this research suggest that students from the TG seemed more aware of educational and career opportunities available to them and appeared readier to grab them. Nevertheless, one should be cautious about touting the ability of NCSSCs to influence young people future career planning, mainly because this is a complicated matter requiring well thought out interventions. For many students, taking relevant career decisions is problematic, as epitomized by the "career-decision making difficulties" literature. According to Gati, Krausz and Osipow's (1996) cognitive decision-making model, there are three major clusters and ten related subfactors that make taking career decisions complicated. In a complementary effort, Saka, Gati and Kelly (2008) created a model to understand career decision-making difficulties taking into account personality and emotional factors; this model featured three major clusters and 11 related subcategories that may degrade career decision-making. The two models' factors are:

Gati, Krausz and Osipow's (1996)	Saka, Gati and Kelly (2008)
Cognitive career decision-making model	**Personality and emotional career decision-making model**
Lack of readiness • Lack of motivation • General indecisiveness • Dysfunctional beliefs **Lack of information (on)** • The career decision-making process • Self • Occupations (i.e., alternatives) • Obtaining information **Inconsistent information (due to)** • Unreliable information • Internal conflicts • External conflicts	**Pessimistic views (about)** • The process • The world of work • One's control **Anxiety** • The process • Uncertainty • The choice • The outcomes **Self-concept and identity** • General anxiety • Self-esteem • Uncrystallised identity • Conflictual attachment and separation

In this context, because career decision making can be so problematic and affected by several of the above factors, researchers have relentlessly worked towards the identification of the most critical elements that make up successful career choice interventions. Whiston and Noblin James (2012) found the following items to be essential:

- Client (i.e. individuals) preferences about the type of career counselling;
- Dose effect, namely the number or the length of career counselling sessions;

- “Critical ingredients” happening in effective sessions: written exercises about occupational analysis and comparison; goal setting and future planning; individualized interpretations and feedback stemming from face-to-face interactions; information about the world of work and specific career options; examples of successful career models; increasing support from schools and families;
- Other process factors.

This limited literature overview on career decision-making difficulties has two major implications.

The first is that it should make NCSSCs’ stakeholders realize that their programme occurs in a context where their participants might have difficulties formulating their career plans, and these difficulties are generated for a variety of reasons that a NCSSS cannot directly influence. For example, while a NCSSC could become a valid provider of information regarding the cyber security profession, it is likely less adept in increasing the motivation or decisiveness of its participants.

The second implication is setting the right expectations on what a programme like a skills competition can achieve. NCSSCs that are serious about increasing career interest should devise sectoral awareness activities that contain the elements listed above. Nonetheless, one should also be aware that NCSSCs have other important objectives, such as increasing cyber security knowledge and skills, which require abundant resources and logistical preparation. Therefore, these programmes should not be expected to fix issues that would be difficult to solve even for more targeted and specialized career interventions.

9.4.2 Key education and career choices

Because this research was delayed three months by Covid-19, it was able to partially investigate the extent to which the CCIT influenced key education and

career choices: 29% of the respondents to the second survey (N=390) had changed their status[52] when they completed the post-participation survey in October 2020 and 49% of them stated that the CCIT had either influenced or partially influenced their choices (section 7.4). In the context of the cyber security skills shortage, one can regard the influence of the CCIT to have been "positive": these students either enrolled in computer science bachelor's degrees to subsequently enrol in cyber security courses, or enrolled in cyber security master's degrees/related master's degrees intending to follow cyber security classes, or started a cyber security job.

While there are some limitations to these findings,[53] they can be considered encouraging. These results mean the CCIT could potentially influence half of its recruits and steer them towards the cyber security sector. In the context of the CCIT, or of other NCSSCs with a similar admission process and requirements, this should not be taken for granted as the programme mainly recruits highly competent computer science generalists and not young cyber security enthusiasts. If almost 50% of them have their education and career choices shaped by the CCIT, one should be satisfied as "actual" education and career choices are by far more substantial evidence of the impact of a NCSSC than the concept of interest. As I will argue in the next section, the concept of interest alone is limited in our understanding of a NCSSC's impact, mainly because 1) when students state they have an interest in a topic or a career, it does not automatically mean that this interest will persist and will develop further, for example by taking relevant key education and career choices; 2) students have other competing interests which are on different "preference levels." Therefore, "actual" education and career

[52] Changing status means either graduating from high school and enrolling in a university bachelor's degree, or enrolling in a master's degree; or looking for employment/start working.
[53] The first is the limited number of students who changed their status (N=110), which is low compared to the number of people who responded to the survey (N=390, only 29%) and very low compared to the number of people who signed up to the CCIT (N=4454). Moreover, it is unknown how many CCIT participants changed their student or employment conditions overall, so it impossible to know how reflective these findings are of the whole population.

choices provide much stronger proof of the influence of a skills competition and should be integrated into the assessment of NCSSCs that are aimed at the CSSS.

Similarly to career decision-making, however, one should not assume that skills competitions will impact the selection of degrees and careers. Indeed, whereas a NCSSC can be reasonably expected to influence topic and career *interest*, it may be unrealistic to ask it to influence education and career *choices* to the same extent, mainly because career choice is complex and based on several factors. The literature review noted that several variables could push people to take one decision or another: Akosah-Twumasi et al. (2018) found that 12 major factors guide youths' key decisions, including:

- financial remuneration,
- job security,
- professional prestige,
- job accessibility,
- personal interest,
- self-efficacy,
- outcome expectations,
- professional development opportunities,
- family members,
- teachers/educators,
- peers,
- social responsibilities.

Whereas research found that the CCIT could influence participants' decisions based on their competition experience, stakeholders should have realistic expectations about what NCSSCs can achieve as these events, very simply put, do not have a bearing on other crucial variables, for example, financial remuneration, job security and professional prestige. This implies that even when a skills competition succeeds in steering participants towards the cyber security sector, individuals might decide to take different career paths if other factors (i.e. low financial remuneration, little professional development opportunities, etc.) work against this decision.

Following up on the analysis in section 9.3.2, an important question on the ability of a NCSSC to influence key education and career choices relates to the issue of timing. As previously noted, the career awareness activities put forward by the CCIT did not seem to have enticed students because they did not come at the right time of their career decision-making. As interviewees were instead more focused on their studies than looking for job opportunities, the CCIT came prematurely in the process and was, therefore, less well-placed to alter these key decisions. On the other hand, it influenced the decisions of about half of those participants who were transitioning from one point to another in their academic or professional careers. The main implication is that those organizing NCSSCs should put some serious thought into the target group they should recruit in order to maximize their outcomes. If the objective of a competition is to take full advantage of its influence on education and career choices, recruiting those individuals that are in the process of taking such decisions could probably have more chances of success than a competition that attracts a broader audience and with more generic objectives. In other words, a NCSSC seeking to increase the number of students enrolling in cyber security master's degrees could target, for example, only final year computer science undergraduate students, and see whether these students enrol in cyber security-related degrees at the end of the skills competition. A NCSSC that adopts this sort of recruitment mechanism may have better chances to influence key decisions than a competition that also recruits first and second-year undergraduate students, who may enjoy the programme, but then develop different interests as they carry on with their studies.

There is no correct answer as to what approach NCSSCs should take as both have their pros and cons. A more "targeted" competition with more limited objectives is probably more likely to achieve them at the expense of being less inclusive and reaching a smaller audience. A more generic and comprehensive competition might have to compromise on its outcomes, but it certainly has an ampler reach. While this is also contingent on budget and resources available, the bottom line is that the timing and target group are paramount when designing a NCSSC and

understanding its effects on complex outcomes such as education and career choices.

9.4.3. Competing interests and the “interest paradox”

A significant finding on the concept of interest and its relationship with skills competitions was that most students had other interests instead of cyber security. I call these “competing interests” as they often seemed to vie for influence in participants’ minds.

It was evident that students had interests that sat alongside cyber security: only 16% of respondents to the second survey (N=390) reported they would rather stay within the cyber security sector; 51% declared there were other topics and careers they were interested in at the same level; 25% said there were other topics and careers that interested them more. Artificial intelligence, generic programming and software engineering were the competing interests CCIT participants were most attracted to (section 7.5). The fact that 84% of participants had educational and career alternatives to cyber security is probably due to the admission process. As the CCIT did not ask for prior cyber security knowledge and skills, and tested generic logic and programming skills, it recruited people with broader interests and career options, despite the programme being centred around cyber security.

These results appear to resonate with findings from the UK Cyber Discovery study, even though Campbell-Jack and colleagues did not elaborate much upon them. They suggested that Cyber Discovery participants were more interested in generic computer science than cyber security before and after the programme. Moreover, the number of students who were “very interested” in computer science grew by 5% from pre to post programme, whilst the number of students interested in cyber security decreased by 10% (even though none of these changes was statistically significant). They suggested:

> “One hypothesis consistent with the tentative evidence to date is that Cyber Discovery may have made some young people aware of the actual nature or requirements of a career that they may not otherwise have known about…This fits with evidence suggesting that participants are interested in a variety of different subjects and careers at this stage…” (2021a, p. 57).

The main implication of this result is that stakeholders should be careful when adopting interest as their unique outcome variable if they wish to fully understand NCSSC impact on the shortage. This occurs because participants may enter the programme being attracted to different topics and careers in addition to cyber security. For example, a student might enter an NCSSC interested in cyber security and software engineering but might actually be more interested in the latter. Hence, even if a NCSSC increases interest in cyber security, a student might still be more interested in software engineering at the end of the programme. We would then have an “interest paradox” whereby a NCSSC could achieve the objective of increasing interest among participants, but it would fail to deliver the intended impact as a student would still be more likely to pursue a software engineering career. The case of a TG student was emblematic and explicative of this paradox. In the post-participation interview, the student explained that his interest in cyber security had grown by 1,5 points due to his CCIT experience, suggesting that the programme had successfully reached its objective. However, he added that during the summer, at the end of the training programme, he had started learning more and more about artificial intelligence to the extent that he felt his interest in AI was now more significant than in cyber security. He concluded that he was now keener to pursue an AI education and professional career rather than one in cyber security. This example clarifies that if one gauges NCSSCs only through the concept of cyber security interest, one may think that the programme's objective was met. Nonetheless, this case study makes it evident that one should embrace a more comprehensive viewpoint and include the perspective of competing interests in the analysis.

9.4.4 Is *interest* still valid to gauge the impact of skills competitions?

To conclude, this section argued that stakeholders should integrate other outcome variables in their NCSSCs' assessment. In the context of the shortage of cyber security professionals, educational and career planning, key choices and competing interests provide harder evidence of what a skills competition may achieve to increase the inflow of young specialists into the cyber security sector.

However, participants enter NCSSCs with competing interests, which are likely to be at the same level, if not superior, than cyber security; young people notoriously have difficulties in planning and taking career decisions, and these difficulties are associated with factors that have little to do with a skills competition; finally, key education and career choices are shaped by variables that a skills event cannot manipulate. Therefore, stakeholders should be realistic about what NCSSCs programmes can actually achieve when these other variables are included in the final assessment.

While results of the CCIT against these outcomes were mixed, this section does not imply that it was ineffective as a shortage mitigation policy. The rest of this chapter has already argued the opposite. The main takeaway of this section is that NCSSCs have to be extremely clear about their goals. If their goal is to "only" influence cyber security interest, they can be organized and implemented similarly to the CCIT. However, if they wish to increase interest in cyber security more than in other competing topics, decrease career decision-making difficulties and make participants enrol in cyber security degrees or apply for cyber security jobs at the end of the event, competitions should add an improved suite of activities (i.e. more targeted career activities, better timing of the intervention etc.) that can help them achieve these enhanced aims. However, stakeholders should also remember that outcomes such as future planning and career choice are based on factors that NCSSCs cannot really manipulate.

Because of these reasons, *interest* is still a reliable indicator to assess a competition, as well as its usefulness in the mitigation of the shortage. It is still

valuable as it provides a “bare minimum” that NCSSCs can effectively influence with solid cyber security training, competent and helpful instructors as well as well-structured and inspiring career awareness activities. Although interest may not be the best indicator to show what an NCSSC actually achieves in augmenting the number of professionals, it is a good indicator of how participants evaluated the programme and how they view cyber security as a subject and career opportunity.

In the end, as already argued in section 9.2 on the establishment of a broader cyber security interest development system, a NCSSC cannot achieve alone what a concert of policies might. Nonetheless, if a NCSSC could effectively trigger interest and positively influence it, it would lay a strong foundation for other policies to further steer students into the cyber security sector.

10. Conclusions

This chapter concludes this thesis by:

- providing a holistic final summary in order to see the big picture (10.1);
- presenting limitations regarding the causation claims on the CCIT's effect on interest and other variables, the choice of interviewees and difficulties in the generalization of findings (10.2);
- offering broader considerations in relation to recent advancements in cyber security skills shortage research as well as suggesting that continued research into this strand of research would benefit relevant debates on skills issues, the future of education and the geopolitics of skills (10.3).

10.1 Final summary

There is a lack of cyber security professionals in the labour market, the so-called cyber security skills shortage (CSSS). There is ample evidence of it, especially if one analyses data coming from specific national labour markets. Cyber security is fundamental for the stability and development of information societies, which are heavily reliant on systems, networks and data. However, cyber space is constantly under attack from multiple threat actors whose goals and actions risk undermining its resilience. Because the absence of such a specialized workforce constitutes a threat to national security and economic development, governments have implemented policies to mitigate the CSSS. NCSSCs have been established with the intent to increase participants' interest in cyber security. Governments hope that, by increasing their cyber security interest, students will enter the cyber security workforce.

However, evidence from the extant literature is mixed and has several knowledge gaps. Among all skills issues, shortages have the least-developed evidence base as scholars have been researching their incidence rather than policies and programmes that could remedy them. The literature on interest is vast, but it lacks

content specificity, and it is still unclear how the relationship between interest development and vocational interest is structured. Research on skills competitions is sparse, and it is still unknown what specific factors within such programmes could cause participants' to become more interested in cyber security. Finally, there is a nice literature on the association between skills competitions and interest, but it has several drawbacks: it is uncertain whether competitions influence participants' interest as so far studies have presented opposing results; much more attention has been devoted to the concept of interest in a career rather than interest in a topic/subject; finally, methodological limitations undermine the validity of these findings.

Against this backdrop, this study aimed at answering three main research questions:

1. How do participants develop an interest in cyber security before joining a NCSSC? What specific factors may trigger the development of cyber security interest?
2. Do NCSSCs influence participants' interest in cyber security? If this is the case, what elements contribute the most to influence it?
3. Ultimately, are NCSSCs an effective policy to address the shortfall of cyber security professionals in the labour market?

This thesis contributed to both theory and practice with its findings on triggers of cyber security interest. It contributed to theory as there had been no specific investigation on how cyber security interest could be initiated and maintained, adding content-specificity to the concept of interest development. However, it also contributed to practice as it identified the specific cyber security factors that could be employed in a broader system of interest development, which can be implemented to create a sustainable national cyber security workforce. This research highlighted that three factors are critical to eliciting interest in cyber security: curiosity, formal and informal coursework, and an NCSSC. Realizing that a NCSSC could trigger cyber security interest was perhaps the most surprising result as it was hypothesized that the high-level entry requirements would prevent

prospective students from becoming interested in it. On a very practical level, the role of a NCSSC as an interest “trigger” means that stakeholders should invest resources in a well-articulated recruitment and marketing strategy in order to ensure that the broadest audience possible is aware of such a skills programme.

Moreover, this study argued that a NCSSC could become the cornerstone of any cyber security interest development system if it manages to meaningfully engage all the participants that it successfully recruits. Such a system would also benefit from including cyber security education in secondary and higher education curricula because of its potential nationwide reach and ability to channel students’ interest into a formal educational path. Finally, this research has warned that creating such an advanced system of interest development risks being derailed unless employers do not collaborate in smoothening the transition from the education system to the labour market.

Furthermore, most respondents to the second survey stated that the CCIT had increased their interest in cyber security as a topic and as a career option. Qualitative findings explained that, while the CCIT was the main reason cyber security interest increased for students in the treatment group, it was instead a co-factor for students in the control group. These results are important as they go against what was hypothesized at the onset of this research, which stated that cyber security interest in the whole CCIT population would have overall decreased. This did not occur because, when students were not admitted to the programme, their disappointment did not grow to the extent they gave up on cyber security and because the CCIT admitted computer science generalists, rather than young cyber security specialists, whose interest in cyber security could be further shaped by the CCIT.

An important contribution of this thesis is being able to explain how the CCIT was able to shape interest among the students who attended the programme, which occurred through the three-month cyber security training. The obvious implication is that NCSSCs should include comprehensive cyber security training rather than merely recruiting participants and making them compete in skills challenges. This

is an essential implication as not many NCSSCs around Europe currently offer cyber security training. Another important finding on the relationship between skills competition and interest was that participants tended to differentiate between interest in cyber security as a topic and interest in cyber security as a career. This is also a significant contribution to interest theory as it suggests that vocational interest may ensue only when interest is well developed. While more research is needed to understand which characteristics and what actions a learner shows and undertakes when vocational interest emerges, this result has a clear and immediate implication for NCSSCs: if participants start a competition with a lower interest in a cyber security career or simply it is generally harder to accrue it, more efforts should be put to ensure participants start thinking more actively of a profession in the cyber security sector.

Additionally, this thesis put in perspective the concept of interest vis-à-vis other outcome variables, such as educational and career planning, key education and career choice, and competing interests. This was possible due to a delay imposed on this research by Covid-19.

It found that CCIT participants appeared to have little awareness of the cyber security sector and available educational and professional opportunities, showing what the literature refers to as “career decision-making difficulties.” This finding reinforces the idea that interest in cyber security as a topic does not equal vocational interest in cyber security and demands further exploration.

Results showed that the CCIT appeared to have influenced almost 50% of participants who took “key” education and career decisions after the CCIT. This influence seemed “positive” as most of the students took decisions that brought them closer to the cyber security sector. This finding is certainly promising as “career choice” gives much more robust evidence of a NCSSC’s influence compared to interest and educational/career planning. This result also underlines the importance of timing, namely at what point of a career-decision making process a skills programme should take place.

Lastly, this research discovered that even participants to the CCIT had competing interests, which meant they were attracted to subjects and careers in other domains and fields, most notably artificial intelligence, software engineering and general programming. The main implication is that NCSSC organizers should not adopt cyber security interest as their sole outcome to avoid facing the “interest paradox.” The interest paradox occurs, for instance, when one student enters a NCSSC interested in cyber security and software engineering, but she is actually more interested in the latter. Hence, even when a NCSSC increases her interest in cyber security, the student might still be more interested in software engineering at the end of the programme. We would have an interest paradox because a NCSSC would have achieved the objective of increasing interest in the student, but it would have failed to deliver the intended impact as she would still be more likely to pursue a software engineering career.

Despite these findings, however, one should consider the concept of interest as a reliable NCSSC’s outcome simply because future planning and career choices are variables that depend upon various factors that a NCSSC cannot manipulate. Therefore, cyber security interest should still be maintained as it is a helpful way to depict how participants evaluated a NCSSC and view cyber security more in general.

To conclude, I argued that a NCSSC organized and implemented like the CCIT could be an effective policy instrument to mitigate the shortfall of cyber security professionals if:

1. It is a component of a broader cyber security interest development system, which should feature the inclusion of formal cyber security coursework in secondary and higher education curriculums. Moreover, a NCSSC could become the cornerstone of such a system if it manages to “meaningfully engage” all its participants.
2. It organizes and implements comprehensive cyber security training and elevates cyber security career awareness activities to higher standards,

following examples from already established career interventions. As it is difficult to shape career decision-making and choice, these activities require the same expertise, resources and time as cyber security training and challenges.

3. It integrates other relevant outcome variables, most notably educational and career planning, key career choices, and “competing interests” when assessing their influence. The latter is especially important to avoid slipping into the “interest paradox.”

It should be underlined that, on its own, a NCSSC is unlikely to achieve what a policy system of cyber security interest development might in dealing with the shortage. As the shortage is an issue with several roots, there are limits to what an NCSSC alone can do. Nonetheless, if such an intervention effectively triggers interest and exerts a positive influence on it, it would lay a strong foundation for other policies to further push students into cyber security.

Furthermore, this thesis made important contributions to interest theory as:

1. It provided content-specificity, identifying the primary triggers that elicit interest specifically in cyber security. Further research should verify whether these factors may trigger interest in other subject areas.
2. It found that participants differentiated between interest in cyber security as a topic and as a career. This implies that more research should be undertaken to understand when vocational interest emerges as a result of interest development in a specific topic.

10.2 Limitations

As with any research, these findings come with a series of limitations. The following sections will discuss limitations regarding this thesis’s causation claims, the absence of interviews conducted with other stakeholders, and difficulties in generalising these study results.

Causation claims

The first limitation of this thesis regards the causation claims on the influence of the CCIT on participants' cyber security interest. Initially, the research design foresaw a quantitative analysis based on a Difference-in-Difference (DiD). Based on data collected from the control and treatment groups, the DiD should have better captured the extent to which the CCIT had changed cyber security interest. However, and although the second survey acquired 390 responses, the number of replies from the control and treatment groups did not reach the required sample size to compare the two groups according to social science standards.[54] Because results based on such analysis would not have been representative, it was decided to concentrate on other methods and data. Therefore, evidence of the influence of the CCIT mainly came from two items of the second survey, which directly asked participants about the "effect" of the CCIT, and pre and post interviews.

While the lack of the DiD analysis restricts this thesis' causation claims, findings should be considered reliable for two reasons. First, the influence of the CCIT was assessed quantitatively through two items in the second survey, which is representative of the whole CCIT population, if responses are not split according to groups. In fact, these survey questions were answered by 390 respondents, a sample size that is representative of the whole CCIT population.[55] While a comparison between control and treatment groups is less solid because of representability issues when considering data according to groups (as explained above), it still gives us a valuable indication of the potential influence of the CCIT on participants. Moreover, the literature on skills competitions and interest features plenty of studies that conducted only post-programme assessments with similarly-phrased survey items (Bashir et al., 2015, 2017; Dabney et al., 2012; Dunn & Merkle, 2018; Miller et al., 2018; Wee et al., 2016).

[54] 95% C.L and +/- 5% margin of error.
[55] For 95% C.L and +/- 5% margin of error taking into account the whole CCIT population (N=4454).

Second, this research features an extensive qualitative component based on 50 interviews – both before and after the CCIT and with participants from different comparison groups – which validated quantitative results and provided further insights. Indeed, the importance of qualitative research for casual explanation in education has been underlined by Maxwell. He argued that "realist" theory,[56] by abandoning the Humean restriction of our understanding of causation, concentrates on identifying the process that results in a specific outcome in a particular context. Therefore, this approach 1) situates process as a central aspect of causation; 2) makes context intrinsic to casual explanation; 3) extends casual explanations to beliefs, values, intentions and meanings. He eloquently concluded that:

> "The idea that randomized experiments or structural equation models can provide valid general conclusions about the effect of an intervention, in the absence of any understanding of the actual causal processes that were operating, the specific contexts in which these processes were situated, or the meaning that the intervention and contexts had for participants, is an illusion. We need qualitative methods and approaches in order to understand "what works" and why" (Maxwell, 2012, pp. 658–659).

Therefore, having dedicated an entire chapter to the CCIT process and several other parts to the context, this study can advance its causation claims regarding the influence of the CCIT on participants while acknowledging its limitations.

Choice of interviewees

Another relevant point, and perhaps limitation, could be the absence of the voice of other stakeholders in this thesis, namely policymakers, organizers, instructors and sponsors. Critics can argue that stakeholders' appraisals could have indeed increased the understanding of CCIT's processes and the context, therefore improving our understanding of its outcomes. While this argument is valid, there are five reasons this study did not include other actors' accounts.

[56] Also known as "generative" or "process" theory.

First, the choice to involve only CCIT participants stemmed mainly from the research objectives of this thesis and was reinforced by a consideration made by the DuVE suite of projects. These projects showed that, while vocational systems as a whole are the primary beneficiaries of these skills events, competitors “sit at the centre” of these communities (Chankseliani, 2015; James Relly & Keep, 2019; Nokelainen & Stasz, 2016). As CCIT participants were also the main protagonists of the Italian NCSSC, their experiences had to be extensively surveyed in order to reach this thesis’ objectives.

Second, and related to the previous point, as this research needed extensive accounts from participants, adding more interviews from stakeholders whose views may have been tangent to this study goals would have meant spending more time perusing extra data. As interviews are time-consuming, this would have been prohibitive within the timeframe of a doctoral study, especially considering that this research had already been delayed by Covid-19.

Third, processes and contexts were thoroughly investigated during interviews with participants and further explored through desktop research. In fact, the CCIT had extensive material about the programme on its website and a vibrant social media ecosystem whose online posts gave further relevant information to direct this study.

Fourth, this thesis was not an evaluation study per se, whose goal was to give the amplest account possible of the CCIT in all its aspects. Instead, this thesis was a doctoral research with specific goals and a more limited approach compared to an encompassing programme evaluation. As this study was also meant to contribute to existing interest theory, the overall scope had to be circumscribed compared to a holistic evaluation.

Last but not least, there was the worry that, by interviewing other actors about participants’ cyber security interest, they would have conflated the extent to which the CCIT was responsible for any change in their interest. This may have occurred not because of any malicious intent but rather for their eagerness to show the benefits of the skills programme. Moreover, the evidence provided would have

been anecdotal rather than systematic. As the literature on skills competitions and interest had mixed results, data collection and analysis had to be more systematic and centred on the very people whose interest was supposed to be shaped, namely CCIT participants.

Generalization of findings

A third important acknowledgement, and perhaps a limitation for some, is that this thesis' findings should be generalized with caution. This holds true simply because, at the moment, the CCIT is very different in comparison to any other NCSSC currently being organized. The literature review found that cyber security skills competitions vastly differ depending on many factors, including size, length, content and type of competition etc. (Conti et al., 2011; Eagle, 2013; van Rensburg & Baker, 2021). Even within Europe, and even though their participation in the ECSC may imply similar objectives and outcomes, NCSSCs are different in several crucial categories, such as length, size, entry requirements, admission process, presence (or not) of training, type of skills challenges and other elements. (De Zan & Yamin, 2021). As competitions are so dissimilar, suggesting that results from the CCIT could be applied to other skills programmes would mean ignoring how various factors affecting skills competitions could alter their outcomes. For example, this thesis found that the three-month cyber security training was the main factor shaping cyber security interest among participants. A comparative analysis of NCSSCs around Europe showed that many NCSSCs currently do not offer training (De Zan & Yamin, 2021). Then, it is plausible that these training-less competitions would be influencing cyber security interest differently, if they do it at all. In a different example, this research found that the CCIT was able to shape interest because it recruited computer science generalists who had varying cyber security experiences, with some of them having no prior exposure. This implies that a NCSSC that recruits mainly young cyber security specialists right from the beginning could be less proficient in shaping their interest, as their attraction to cyber security is likely to be already at the highest level. These are just a few

examples based on the findings, but many more could be added to show how the different facets of a competition could produce vastly different outcomes.

In this context, one should also consider how the broader educational, professional, and cultural context in which skills competitions take place may have a role in influencing NCSSCs' outcomes. For instance, it is uncommon for Italian students to be looking for placement opportunities during their undergraduate studies, and undertaking them even rarer, which seems in contrast with what happens in Anglo-Saxon countries, where accumulating professional experience during university years is almost a given. Hence, one could wonder what the effects of an intervention encouraging Italian undergraduate students to pursue such placements could be, unless the broader context makes them realize that doing so is not only acceptable but perhaps desirable.

To conclude, this paragraph was intended to underline that these research findings could be hard to generalize in light of NCSSCs' differences. This implies that each NCSSC should be investigated independently rather than assuming that, simply because these programmes share the same name and often analogous features, they produce the same effects.

10.3 Broader considerations

When I was preparing my research proposal for admission to this DPhil in the fall of 2016, I realized the cyber security skills shortage (CSSS) was one of a kind among all topics one could choose to write a thesis on. The main issue was that everyone was talking about it in various forms and venues, but scientific inquiry had not yet weighed in. The absence of a solid body of background research on the topic made the writing of the research proposal a particularly challenging task. The overall lack of systematic studies was confirmed later when I undertook a more rigorous literature review, which found that among all skills issues, shortages are those with the least developed evidence basis (McGuinness et al., 2018). The problem was even more acute for sector-specific shortages such as cyber security.

Since 2016, there have been some steps forward in studying the CSSS, but perhaps not as much as one would have liked to see, given the issue's prominence.

In terms of improvements, the CSSS has consolidated as an area of attention, and interested stakeholders have continued debating it. The issue is regularly cited in countries' strategic cyber security documents (Nurse, Grammatopoulos, Adamos, & Di Franco, 2021); information security industry associations have kept publishing their yearly updates on the status of the cyber security workforce ((ISC)^2, 2020; ISACA, 2021; Oltsik & Lundell, 2021) and there are often online articles and analyses reminding us of the need to do something about it (Xie, 2019). The fact that the CSSS has not disappeared from the policy radar is a positive sign as it means stakeholders still consider it as a topic worth of discussion and, perhaps, action.

Moreover, the awareness that the labour market (i.e. employers) has a role in creating a solid cyber security workforce is an emerging theme. For example, Vinberg stated that "many organizations are looking for the wrong thing in the wrong places and blaming newcomers for it. (…) Once it becomes clear that off-the-shelf experts aren't realistic at scale, cultivating entry-level talent emerges as the only long-term solution — not just for a hiring organization but for the field as a whole" (Vinberg, 2020). Reiterating this new awareness, in November 2011, Microsoft declared it was launching a campaign to help skill and recruit 250,000 people into the US cybersecurity workforce by 2025 (Smith, 2021). This is a welcome turn in the debate on the CSSS, which has long suffered from the biased perspective of employers and their single-sided viewpoints about the inability of the education system to "produce" cyber security professionals. In this context, it is important for employers to further realize that 1) the education system is not meant to generate "ready-to-use" cyber security professionals. To quote a human resources and management expert that I interviewed for background research to this thesis, "It is extraordinarily difficult for academic institutions to provide work experience: creating pretend experience does not work well. Employers have to

do it, but how we encourage them to do so is something we do not really know" (De Zan, 2019a, p. 73); 2) employers should not passively sit at the receiving end of the demand-supply curve and hope their cyber security workforce will increase their knowledge and skills on their own; instead, they must adopt a pro-active role in shaping it through various means, including entry-level placements, training opportunities and adequate salaries and work environments. Even though powerful private sector companies might have the resources to address their internal skills shortages on their own, employers should not be left alone in finding solutions for an issue with multiple roots. A collaboration among multiple stakeholders, or to use a concept currently in high-fashion, a "public-private partnership" (PPP) is better suited to tackle an issue requiring different actors and tools to cope with it. However, this collaboration can only start when employers realize their importance and role in establishing a cyber security workforce, and this recent shift in attitude is an encouraging step towards creating more balanced and effective PPPs.

Another exciting evolution has been the policy developments in some countries, in particular in Australia and the UK. As I could closely monitor developments in the UK, I will briefly explain why HM Government's policies in this area constitute a significant advancement. In a book chapter on cyber security education policy (De Zan, 2021), I explained that two efforts would have been particularly welcomed to advance knowledge and practice in the field: 1) gathering more compelling evidence about the incidence of the CSSS at the national level; 2) understanding what works and what does not in skills shortage policies. I argued this because evidence of the shortage was based on industry reports and anecdotal evidence and because, notwithstanding many countries had in place policies to tackle it, governments did not seem to know the effects of their programmes. The UK is perhaps the only country that has improved in both areas. For example, on the incidence of the shortage, since 2018, the UK government has sponsored very detailed analyses of the cyber security labour market (McHenry et al., 2021; Pedley et al., 2020; Pedley, McHenry, Motha, & Navin, 2018), including thorough investigations of the supply side (Malan et al., 2018; Williams et al., 2021). UK

analyses punched above their weight as they included data and indicators that had not been included in previous national analyses, providing a wealth of information that any country should parallel if they are serious about the CSSS challenge.

Furthermore, the UK is probably the only country that has dedicated a separate policy document for cyber security education and skills policy, the “Initial National Cyber Security Skills Strategy: increasing the UK’s cyber security capability” (HM Government, 2018a). The document contains a detailed list of rationales and policies according to different types and levels of intervention (i.e. primary and secondary education, higher education, the labour market etc.), probably including the most comprehensive array of programmes ever put in place by a government to tackle the shortage. What is also vital is that London understood the importance of evaluating these programmes and recently funded independent studies to assess their impact (Campbell-Jack et al., 2021a; Campbell-Jack, Bickley, & Lillis, 2021c; RSM, 2020c, 2020d, 2020a). In sum, this comprehensive approach to the CSSS is an important advancement, making the UK a unique case study for all other countries attempting to grapple with the same problem.

While these improvements are welcomed, one may wish more had been done in the past five years. On the incidence of the shortage, apart from research in Anglo-Saxon countries, analyses in other national markets are still lagging. Reports from information security associations continue to drive the debate, even though their methodologies have not improved as they should have. Countries have promoted cyber security and awareness policies and cited them in their strategic documents, but they are at times so vague that one is left wondering what these programmes have achieved in practice. Policy organisations still focus too much on the supply side of skills (Nurse et al., 2021; Organization of American States, 2020) rather than creating stronger PPPs where employers are more closely integrated into solving the CSSS. Since their inception in 2015 and 2016, the two most relevant scientific outlets on the social science and policy aspects of cyber security, the Journal of Cybersecurity and Journal of Cyber Policy, have published only one

article on CSSS issues.[57] In general, there are still many “dilemmas” surrounding cyber security education and skills policy that should be faced (Austin, 2021).

Hence, continued research into the cyber security skills shortage would benefit knowledge and practice. I contend there are three main areas that could benefit from extended research: skill issues, the future of education, and the geopolitics of skills. Each of them is addressed below.

Skills issues

Further studying the CSSS would help hone our ability to deal with shortages more generally. In fact, there is a lot to learn from a specific sector shortage, such as the one in cyber security. Perhaps the first lesson learnt regards the need to ascertain its incidence. The literature is clear about it: it is difficult to prove when shortages are genuine and not being talked up by employers. Therefore, knowing the contours and nature of the problem is a central part of the process. Some recent shortage investigations have reached a good level of sophistication thanks to the inclusion of batteries of indicators and multiple methods of data collection and analysis (AustCyber, 2018; McHenry et al., 2021; Williams et al., 2021). The bottom line is that advances in the investigation of the incidence of the CSSS could be used to find out whether shortages in other sectors are happening and avoid falling into simplistic versions of employer-driven skills shortage rhetoric.

The second element that one could learn from the CSSS is the need to break down the problem into smaller issues and refine research questions. The CSSS is an umbrella term that has been used to describe all sorts of issues at the intersection between cyber security supply and demand. Nonetheless, in order to address these issues scientifically, research needs to correctly identify where the locus of the problem is. We know there are currently various factors compounding the CSSS, and these could reside within both supply and demand. However, one

[57] The article in question is “Cybersecurity education in a developing nation: the Ecuadorian environment” (Catota, Morgan, & Sicker, 2019).

needs to define where the problem is in order to devise the correct solution. For instance, if the problem is the number of students entering the pipeline, a country may establish as many cyber security master's degrees as possible, but if students do not enrol, the CSSS will not be mitigated. Likewise, one can have the most expansive pool of cyber security graduates available, but if employers are looking for professionals with five or more years of work experience, there will be again a disconnection between the policy established and the one that is needed. Therefore, correctly identifying where the problem lies can also be transferred to other sectors where the terminology "skills shortage" does not help identify the actual issue.

Finally, research into policy programmes such as cyber security competitions can also yield interesting results in other sectors: if there was a shortage of artificial intelligence professionals, would a competition such as an NCSSC increase interest in the subject? What adjustments would be necessary? If it is true that research on shortages has not been focusing on policies (CEDEFOP, 2015), research such as this thesis or the UK government's independent evaluations could help steer programmes in other sectors without having to start from scratch.

To conclude, the labour market will likely be transformed by innovation in artificial intelligence, automation and further connectivity (Frontier economics, 2018; Petropoulos, 2021). As the nature of work will require newer knowledge and skillsets, its workforce will have to be equipped with those. Further research into skills imbalances, especially shortages, can give insights into doing it more efficiently.

The future of education and OST programmes

One could wonder whether this research also tells us something about the future of education as well. There is much discussion on what this future is going to look like, with influential authors listing at least four different scenarios: 1) schooling extended, where participation in formal education continues to expand; 2)

education outsourced, where education takes place in more diverse, privatised and flexible arrangements and where technology is a key driver; 3) schools as learning hubs, where the role of the school is central, and it is the fulcrum and connector of new forms of learning, civic engagement and social innovation; 4) learn-as-you-go, where education takes place everywhere and anytime and with no distinctions between formal and informal learning (Schleicher, 2021).

Against this backdrop, this research highlighted some of the tensions that the future will reserve for the education sector. Results showed that NCSSCs increased interest in cyber security thanks to the training. Instilling knowledge is what formal education institutions are tasked to do, but study participants lamented the fact that the type of education provided by these institutions was often too theoretical, which left them unprepared when facing real-world challenges. Many of them solved this conundrum by learning on their own the topic they were interested in. This is not surprising as Out-of-School Time activities (OSTs) are much more agile than formal educational institutions, which require time when enacting changes to curricula, formats and structures (even though Covid-19 showed how quickly changes could be made when these are needed to ensure continuity in the advent of difficulties). These programmes also provide learning in a different setting from traditional classrooms, which is a venue that some students might find less enticing. OSTs also have the benefits of being designed by multiple stakeholders: when stakeholders from multiple areas convene to design a programme like NCSSCs they bring various perspectives, methodologies and resources that formal education systems cannot replicate.

Whilst OSTs such as NCSSCs may represent an alternative to formal education to a certain extent, most likely, they will complement it. As a starting point, it is evident that OSTs, even when implemented at the national level, cannot have the same nationwide reach as formal institutions, as discussed in section 9.2.4. In fact, the CCIT was popular and benefited from an ample recruiting base because the Italian national network of secondary and higher education institutes sponsored it among their students. While often criticized, traditional institutions were always

present, perhaps in the background, even during the CCIT. Formal learning and key figures such as teachers and professors had a role in triggering interest in technology and cyber security, which motivated students to sign up for the skills programme. It was also because CCIT tutors, namely university academic staff such as professors, researchers and doctoral students, were so prepared and helpful that students enjoyed the programme. Whereas students depicted formal learning environments as limiting, the CCIT would have taken place in the very same university classrooms where students felt bored at times if Covid-19 had not struck.

To conclude, this section pointed out that the future of education foresees different scenarios, some of them being relatively distant from the current one. OSTs activities such as NCSSCs offer different perspectives on how education could be provided and informed. Hence, deeper integration between these programmes and traditional settings and education methods can provide exciting avenues for innovative learning.

The geopolitics of skills

Finally, I would contend that doing more research in the CSSS is warranted as, so far, it has not been granted the “strategic relevance” it deserves. There are numerous ways that the CSSS could impact economic development and national security. For example, a lack of adequate cyber security in the private sector means companies may lose proprietary data due to hacking, which could cause them to go out of business (Aguilar, 2015). If this happens on a large scale, this could mean economies will suffer because of cyber-related issues in addition to economic ones. Consequences for national security are even more evident. For instance, after sensitive designs of the F-35 Joint Strike Fighter programme were stolen, a top Pentagon official declared that this took away a significant US advantage, severely undermining American superiority in a strategic sector (D. Alexander, 2013).

Some policy institutions are starting to realize the geopolitics of specific sectorial skills, including cyber security. For example, in criticizing the government's slow response to the shortage of security professionals, the UK parliament's Joint Committee on the National Security Strategy noted that the issue was of "vital importance to both national security and the economy" (2018, p. 7). The US government pushed this argument even further when it stated that:

> "America's cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life. The National Cyber Strategy, the President's 2018 Management Agenda, and Executive Order 13800 (…), each emphasize that a superior cybersecurity workforce will promote American prosperity and preserve peace" (The White House, 2019).

If the cyber security workforce is a "strategic asset" that can promote prosperity and preserve peace, this makes the lack of cyber security experts a strategic issue with geopolitical implications. Recognizing this would not mean "securitizing"[58] cyber security education but giving it the place it warrants in stakeholders' minds when they allocate resources to the various items in a cyber security strategy.

Knowing how to deal with shortages in cyber security could help us understand how to minimize shortages in other emerging strategic sectors as well. For instance, there is little doubt that mastering artificial intelligence will have profound economic, societal and strategic implications, to the extent that Russian President Vladimir Putin once said: "Whoever becomes the leader in this sphere will become the ruler of the world" (Gigova, 2017). Therefore, against the backdrop of an emerging shortage occurring even in the AI field (Jarvis, 2020; Russon & Hooker, 2021), stakeholders should be concerned about applying lessons learnt from dealing with "strategic skills shortages," such as in cyber security, to other relevant sectors.

[58] Securitization theory contends that state actors engage in a process of securitization when they elevate a regular politics issue to a matter of "security" (Buzan, Wæver, de Wilde, & Wilde, 1998).

References

(ISC)^2. (2018). *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)^2 Cybersecurity Workforce Study 2018*. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

(ISC)^2. (2020). *Cybersecurity Professionals Stand Up to a Pandemic*. Retrieved from https://www.isc2.org/Research/Workforce-Study

(ISC)^2. (2021). *A Resilient Cybersecurity Profession Charts the Path Forward*. Retrieved from https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Adcock, R. A., Thangavel, A., Whitfield-Gabrieli, S., Knutson, B., & Gabrieli, J. D. E. (2006). Reward-Motivated Learning: Mesolimbic Activation Precedes Memory Formation. *Neuron*, *50*(3), 507–517. https://doi.org/10.1016/j.neuron.2006.03.036

Aguilar, L. A. (2015). The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses. Retrieved October 28, 2021, from U.S. Securities and Exchange Commission website: https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

Aica, Anitec-Assinform, Assintel, & Assinter Italia. (2019). *Osservatorio delle competenze digitali*. Retrieved from https://competenzedigitali.org/wp-content/uploads/2020/01/Osservatorio_CompetenzeDigitali_2019.pdf

Aica, Assinform, Assintel, & Assinter. (2017). *Osservatorio sulle Competene Digitali*. Retrieved from https://www.agid.gov.it/sites/default/files/repository_files/osservatorio_competenze_digitali_2017.pdf

Ainley, M., & Hidi, S. (2014). Interest and enjoyment. In R. Pekrun & L. Linnenbrink-Garcia (Eds.), *International handbook of emotions in education* (pp. 205–227). Routledge/Taylor & Francis Group.

Ainley, Mary, Hidi, S., & Berndorff, D. (2002). Interest, learning, and the psychological processes that mediate their relationship. *Journal of Educational Psychology*, *94*(3), 545–561. https://doi.org/10.1037/0022-0663.94.3.545

Air Force Association. (2019). *Cyber Patriot Impact Report*. Retrieved from https://www.uscyberpatriot.org/Documents/Fact Sheets/Impact Report_sponsor_2019.pdf

Akosah-Twumasi, P., Emeto, T. I., Lindsay, D., Tsey, K., & Malau-Aduli, B. S. (2018). A Systematic Review of Factors That Influence Youths Career Choices—the Role of Culture. *Frontiers in Education*, *3*. https://doi.org/10.3389/feduc.2018.00058

Alexander, D. (2013). Theft of F-35 design data is helping U.S. adversaries -Pentagon | Reuters. Retrieved October 28, 2021, from Reuters website: https://www.reuters.com/article/usa-fighter-hacking-idUSL2N0EV0T320130619

Alexander, P. A., & Murphy, P. K. (1998). Profiling the differences in students' knowledge, interest, and strategic processing. *Journal of Educational Psychology*, *90*(3), 435–447. https://doi.org/10.1037/0022-0663.90.3.435

Ali, M., Talib, C. A., Surif, J., Ibrahim, N. H., & Abdullah, A. H. (2018). Effect of STEM competition on STEM career interest. *2018 IEEE 10th International Conference on Engineering Education (ICEED)*, 111–116. https://doi.org/10.1109/ICEED.2018.8626904

Allport, G. W. (1946). Effect: a secondary principle of learning. *Psychological Review*, *53*(6), 335–347. https://doi.org/10.1037/h0059295

Anderson, B. A., Laurent, P. A., & Yantis, S. (2011). Value-driven attentional capture. *Proceedings of the National Academy of Sciences*, *108*(25), 10367–10371. https://doi.org/10.1073/pnas.1104047108

ANSA. (2020a). Coronavirus: Italy intensifies lockdown measures - English - ANSA.it. Retrieved April 1, 2020, from https://www.ansa.it/english/news/2020/03/12/coronavirus-italy-intensifies-lockdown-measures_5a74bc76-0411-42f3-bf9f-d13cf2302e14.html

ANSA. (2020b). Coronavirus: Italy wakes up in lockdown - English - ANSA.it. Retrieved April 1, 2020, from

https://www.ansa.it/english/news/general_news/2020/03/10/coronavirus-italy-wakes-up-in-lockdown_304a6b61-8a6a-43bb-867c-430c02c79b48.html

Aspen Cybersecurity Group. (2018). *Principles for Growing and Sustaining the Nation's Cybersecurity Workforce*. Retrieved from https://assets.aspeninstitute.org/content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf

Atitsogbe, K. A., Moumoula, I. A., Rochat, S., Antonietti, J.-P., & Rossier, J. (2018). Vocational interests and career indecision in Switzerland and Burkina Faso: Cross-cultural similarities and differences. *Journal of Vocational Behavior*, *107*, 126–140. https://doi.org/10.1016/j.jvb.2018.04.002

AustCyber. (2018). *Australia's Cyber Security Sector Competitiveness Plan - 2018 update - Driving growth in Australia's cyber security sector*. Retrieved from https://www.austcyber.com/file-download/download/public/415

AustCyber. (2019a). Competitions and challenges | AustCyber. Retrieved November 26, 2019, from https://www.austcyber.com/educate/competitions-and-challenges

AustCyber. (2019b). *CyberTaipan Pilot Program Impact Report*. Retrieved from https://www.austcyber.com/resource/cybertaipan-pilot-program-impact-report-20182019

AustCyber. (2020). *Australia's Cyber Security Sector Competitiveness Plan 2020 Update*. Retrieved from https://www.austcyber.com/resources/sector-competitiveness-plan

Austin, G. (2021). Twelve dilemmas of reform in cyber security education. In G. Austin (Ed.), *Cyber Security Education: Principles and Policies*. Retrieved from https://www.routledge.com/Cyber-Security-Education-Principles-and-Policies/Austin/p/book/9780367421915

Australian Cyber Security Growth Network. (2017). *Cyber Security Sector Competitiveness Plan*. Retrieved from https://www.austcyber.com/file-download/download/public/327

Australian Government. (2016). *Australia's Cyber Security Strategy: Enabling innovation,*

growth & prosperity. Retrieved from https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf

Australian Government. (2020). *Australia's Cyber Security Strategy*. Retrieved from https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Azevedo, F. S. (2006). Personal Excursions: Investigating the Dynamics of Student Engagement. *International Journal of Computers for Mathematical Learning*, *11*(1), 57–98. https://doi.org/10.1007/s10758-006-0007-6

Azevedo, F. S. (2013). The Tailored Practice of Hobbies and Its Implication for the Design of Interest-Driven Learning Environments. *Journal of the Learning Sciences*, *22*(3), 462–510. https://doi.org/10.1080/10508406.2012.730082

Bandura, A. (1986). Social foundations of thought and action : a social cognitive theory / Albert Bandura. *New Jersey: Prentice-Hall, 1986*, *16*(1).

Bandura, A., & Locke, E. A. (2003). Negative self-efficacy and goal effects revisited. *Journal of Applied Psychology*, *88*(1), 87–99. https://doi.org/10.1037/0021-9010.88.1.87

Banerji, A., Cunningham, W., Fiszbein, A., King, E., Patrinos, H., Robalino, D., & Jee-Peng, T. (2010). *Stepping Up Skills for More Jobs and Higher Productivity*. Retrieved from https://openknowledge.worldbank.org/bitstream/handle/10986/27892/555660WP0Box341101061141CT01PUBLIC1.pdf?sequence=1&isAllowed=y

Bashir, M., Lambert, A., Guo, B., Memon, N., & Halevi, T. (2015). Cybersecurity Competitions: The Human Angle. *IEEE Security & Privacy*, *13*(5), 74–79. https://doi.org/10.1109/MSP.2015.100

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, *65*, 153–165. https://doi.org/10.1016/J.COSE.2016.10.007

Bate, L. (2017). The Cyber Workforce Gap: A National Security Liability? Retrieved

September 17, 2019, from War On The Rocks website: https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/

Bate, L. (2018). *Cybersecurity Workforce Development: A Primer*. Retrieved from https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_Workforce_Development_A_Primer_2018-10-31_175830_YMwa3ZJ.pdf

Bell, P., Lewenstein, B., Shouse, A. W., & Feder, M. A. (Eds.). (2009). *Learning Science in Informal Environments*. https://doi.org/10.17226/12190

Bernacki, M. L., & Walkington, C. (2018). The role of situational interest in personalized learning. *Journal of Educational Psychology*, *110*(6), 864–881. https://doi.org/10.1037/edu0000250

Bhaskar, R. (2013). A realist theory of science. In *A Realist Theory of Science*. https://doi.org/10.4324/9780203090732

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2021). Educating future multidisciplinary cyber security teams. In G. Austin (Ed.), *Cyber Security Education: Principles and Policies*. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9780367822576-4/educating-future-multidisciplinary-cyber-security-teams-jean-blair-andrew-hall-edward-sobiesk?context=ubx&refId=a08fd535-7c0d-4708-bb19-125ac2fdb137

Boccellato, P. (2021). Baldoni: “In Italia tra imprese e Pa servono 100mila esperti di sicurezza.” Retrieved December 23, 2021, from Cybersecurity Italia website: https://www.cybersecitalia.it/cybersecurity-baldoni-acn-in-italia-tra-imprese-e-pa-servono-100mila-esperti-di-sicurezza/15720/

Boekaerts, M., & Minnaert, A. (2003). Measuring behavioral change processes during an ongoing innovation program: scope and limits. In *Powerful learning environments: Unravelling basic components and dimensions.*

Boeri, T., & van Ours, J. (2008). Education and Training. In *The Economics of Imperfect Labor Markets* (1st ed.). https://doi.org/10.2307/j.ctt32bc18

Bogdan, R.Biklen, & S.K. (1992). *Qualitative Research for Education: An Introduction to Theory and Methods*. Boston: Allyn & Bacon.

Bojuwoye, O., & Mbanjwa, S. (2006). Factors Impacting on Career Choices of Technikon Students From Previously Disadvantaged High Schools. *Journal of Psychology in Africa*, *16*(1), 3–16. https://doi.org/10.1080/14330237.2006.10820099

Boyatzis, R. E. (1998). *Transforming qualitative information: thematica analysis and code development*. Thousand Oaks: SAGE Publications Inc.

Boyle, J., Berman, L., Dayton, J., Iachan, R., Jans, M., & ZuWallack, R. (2021). Physical measures and biomarker collection in health surveys: Propensity to participate. *Research in Social and Administrative Pharmacy*, *17*(5), 921–929. https://doi.org/10.1016/j.sapharm.2020.07.025

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brisolara, S. (2018). Outcomes. In B. B. Frey (Ed.), *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*. https://doi.org/10.4135/9781506326139

Brunello, G., & Wruuck, P. (2021). Skill shortages and skill mismatch: A review of the literature. *Journal of Economic Surveys*, joes.12424. https://doi.org/10.1111/joes.12424

Bryman, A. (2015). *Social Research Methods* (5th ed.). Oxford: Oxford University Press.

Buchanan, J., Finegold, D., Mayhew, K., & Warhurst, C. (2017). Introduction: Skills and Training: Multiple Targets, Shifting Terrain. In J. Buchanan, D. Finegold, K. Mayhew, & C. Warhurst (Eds.), *The Oxford Handbook of Skills and Training* (Vol. 1). https://doi.org/10.1093/oxfordhb/9780199655366.013.33

Bunzeck, N., Doeller, C. F., Fuentemilla, L., Dolan, R. J., & Duzel, E. (2009). Reward Motivation Accelerates the Onset of Neural Novelty Signals in Humans to 85 Milliseconds. *Current Biology*, *19*(15), 1294–1300. https://doi.org/10.1016/j.cub.2009.06.021

Burningglass. (2019). *Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring*. Retrieved from https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf

Buzan, B., Wæver, O., de Wilde, J., & Wilde, J. De. (1998). Security: A New Framework for Analysis - Barry Buzan, Ole Wæver, Ole Waever, Jaap de Wilde - Google Books. In *National Bureau of Economic Research Working Paper Series* (Vol. 93). Retrieved from https://books.google.be/books/about/Security.html?id=j4BGr-Elsp8C&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false

Caldera, Y. M., Robitschek, C., Frame, M., & Pannell, M. (2003). Intrapersonal, familial, and cultural factors in the commitment to a career choice of Mexican American and non-Hispanic White college women. *Journal of Counseling Psychology*, *50*(3), 309–323. https://doi.org/10.1037/0022-0167.50.3.309

Campbell-Jack, D., Bickley, H., & Lillis, J. (2021a). *Cyber Discovery Evaluation*. Retrieved from https://www.gov.uk/government/publications/independent-evaluations-of-cyber-discovery-and-cyberfirst-programmes/cyber-discovery-evaluation

Campbell-Jack, D., Bickley, H., & Lillis, J. (2021b). *CyberFirst Evaluation*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1009119/CyberFirst_report_ACCESSIBLE.pdf

Campbell-Jack, D., Bickley, H., & Lillis, J. (2021c). *CyberFirst Evaluation*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1009119/CyberFirst_report_ACCESSIBLE.pdf

Campbell, J.R., Wagner, H., & Walberg, H. J. (2000). Academic competitions and programs designed to challenge the exceptionally talented. In *International handbook of giftedness and talent*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.535.1138&rep=rep1&type=pdf

Campbell, James Reed, & Walberg, H. J. (2010). Olympiad Studies: Competitions Provide Alternatives to Developing Talents That Serve National Interests. *Roeper Review*, *33*(1), 8–17. https://doi.org/10.1080/02783193.2011.530202

Capgemini Digital Transformation Institute. (2018). *CYBERSECURITY TALENT: the BIG GAP in Cyber Protection*. Retrieved from https://www.capgemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf

Cappelli, P. H. (2015). Skill Gaps, Skill Shortages, and Skill Mismatches: Evidence and Arguments for the United States. *ILR Review*, *68*(2), 251–290. https://doi.org/10.1177/0019793914564961

CEDEFOP. (2015). *Tackling unemployment while addressing skill mismatch: Lessons from policy and practice in European Union countries*. https://doi.org/http://dx.doi.org/10.2801/648140

CEDEFOP. (2018). *Insights into skill shortages and skill mismatch: Learning from Cedefop's European skills and jobs survey*. Retrieved from https://www.cedefop.europa.eu/files/3075_en.pdf

Center for Strategic and International Studies. (2016). *Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills*. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

Center for Youth and Communities. (2019). *FIRST Longitudinal Study Technical Note*. Retrieved from https://www.firstinspires.org/sites/default/files/uploads/resource_library/impact/first-longitudinal-study-technical-details-april-2019.pdf

Chankseliani, M. (2015). *WorldSkills and entrepreneurship: a report to the Skills Funding Agency*. Retrieved from http://vocationalexcellence.education.ox.ac.uk/wordpress/wp-content/uploads/2015/06/Project-5-WorldSkills-competitors-and-entrepreneurship.pdf

Charmaz, K. (2003). Grounded theory. In J. A. Smith (Ed.), *Qualitative Psychology: A Practical Guide to Research Methods* (pp. 81–110). London: SAGE Publications Ltd.

Chattopadhyay, S. (2012). Concept of Market and Market Failure in Education. In *Education and Economics: Disciplinary Evolution and Policy Discourse*. https://doi.org/10.1093/acprof:oso/9780198082255.001.0001

Chen, A., Darst, P. W., & Pangrazi, R. P. (1999). What Constitutes Situational Interest? Validating a Construct in Physical Education. *Measurement in Physical Education and Exercise Science*, *3*(3), 157–XXX.

https://doi.org/10.1207/s15327841mpee0303_3

Chen, A., Darst, P. W., & Pangrazi, R. P. (2001). An examination of situational interest and its sources. *British Journal of Educational Psychology*, *71*(3), 383–400. https://doi.org/10.1348/000709901158578

Cheng, H. N. H., Wu, W. M. C., Liao, C. C. Y., & Chan, T.-W. (2009). Equal opportunity tactic: Redesigning and applying competition games in classrooms. *Computers & Education*, *53*(3), 866–876. https://doi.org/10.1016/j.compedu.2009.05.006

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012). *Effectiveness of Cybersecurity Competitions*.

Choi, K., & Kim, D.-Y. (2013). A cross cultural study of antecedents on career preparation behavior: Learning motivation, academic achievement, and career decision self-efficacy. *Journal of Hospitality, Leisure, Sport & Tourism Education*, *13*, 19–32. https://doi.org/10.1016/j.jhlste.2013.04.001

CINI Cybersecurity National Lab. (2019). *CyberChallenge.IT 2020*. Retrieved from https://cyberchallenge.it/assets/CCIT20-sito-EN.pdf

CINI Cybersecurity National Lab. (2020a). CyberChallengeIT: a ottobre la gara nazionale degli hacker etici sarà online - Cybersecurity National Lab. Retrieved August 17, 2020, from https://cybersecnatlab.it/cyberchallenge-it-ottobre-2020-gara-nazionale-hacker-etici-online-covid/

CINI Cybersecurity National Lab. (2020b). CyberChallengeIT: concluse in “smart working” le lezioni degli hacker etici - Cybersecurity National Lab. Retrieved June 9, 2020, from https://cybersecnatlab.it/cyberchallengeit-concluse-lezioni-hacker-etici-smart-working/

CINI Cybersecurity National Lab. (2020c). Il Team Università di Pisa vince la CyberChallengeIT 2020 - Cybersecurity National Lab. Retrieved October 28, 2020, from https://cybersecnatlab.it/team-universita-pisa-vince-cyberchallengeit-2020/

CINI Cybersecurity National Lab. (2020d). OpenCyberChallengeIT, il programma di formazione esteso a 1.300 nuove leve - Cybersecurity National Lab. Retrieved May 12, 2020, from https://cybersecnatlab.it/open-cyberchallengeit-programma-formazione-esteso-nuove-leve/

Coats, D. R. (2019). *Worlwide Threat Assessment of the US Intelligence Community*. Retrieved from https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Cobb, P., & Hodge, L. L. (2003). An Initial Contribution to the Development of a Design Theory of Mathematical Interests: The Case of Statistical Data Analysis. *Communications of Mathematical Education*, *16*.

Cobb, S. (2016). *Mind this gap: criminal hacking and the global cybersecurity skills shortage, a critical analysis*. Retrieved from https://www.virusbulletin.com/virusbulletin/2016/12/vb2016-paper-mind-gap-criminal-hacking-and-global-cybersecurity-skills-shortage-critical-analysis/

Conklin, A. (2005). The use of a collegiate cyber defense competition in information security education. *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development - InfoSecCD '05*, 16. https://doi.org/10.1145/1107622.1107627

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. *2014 47th Hawaii International Conference on System Sciences*, 2006–2014. https://doi.org/10.1109/HICSS.2014.254

Conti, G., Babbitt, T., & Nelson, J. (2011). Hacking Competitions and Their Untapped Potential for Security Education. *IEEE Security & Privacy Magazine*, *9*(3), 56–59. https://doi.org/10.1109/MSP.2011.51

Creswell, J. W., & Creswell, D. J. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). Thousand Oaks: SAGE Publications Inc.

Crumpler, W., & Lewis, J. A. (2019). *The Cybersecurity Workforce Gap*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

CSIS. (2016). *Hacking the Skills Shortage - A study of the international shortage in cybersecurity skills*. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

CSIS Commission on Cybersecurity for the 44th Presidency. (2010). *A Human Capital*

Crisis in Cybersecurity Technical Proficiency Matters. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf

Cyber Discovery. (2019a). About Cyber Discovery – Medium. Retrieved November 21, 2019, from https://medium.com/cyber-discovery/about

Cyber Discovery. (2019b). Cyber Discovery launches the first CyberStart Elite Camp in Manchester. Retrieved November 21, 2019, from https://medium.com/cyber-discovery/cyber-discovery-launches-the-first-cyberstart-elite-camp-in-manchester-f9860b59e7d

Cyber Discovery. (2019c). Year 2. What's new? - Cyber Discovery - Medium. Retrieved November 21, 2019, from https://medium.com/cyber-discovery/year-2-whats-new-4442efd4df8a

Cyber Seek. (2021). Cybersecurity Supply And Demand Heat Map. Retrieved October 12, 2021, from https://www.cyberseek.org/heatmap.html

CyberChallenge.IT. (2019). CyberChallenge.IT. Retrieved September 17, 2019, from https://www.cyberchallenge.it/

CyberTitan. (2019). What is CyberTitan – CyberTitan – ICTC Canadian Youth Cyber Education Initiative. Retrieved September 23, 2019, from https://www.cybertitan.ca/index.php/about/what-is-cybertitan/

Dabney, K. P., Tai, R. H., Almarode, J. T., Miller-Friedmann, J. L., Sonnert, G., Sadler, P. M., & Hazari, Z. (2012). Out-of-School Time Science Activities and Their Association with Career Interest in STEM. *International Journal of Science Education, Part B*, *2*(1), 63–79. https://doi.org/10.1080/21548455.2011.629455

Dainton, F. S. (1968). *The Dainton report: An inquiry into the flow of candidates into science and technology*.

Dan, S., Kohnke, A., & Sigler, K. (2021). What the profession of cyber security needs to know and do. In G. Austin (Ed.), *Cyber Security Education: Principles and Policies*. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9780367822576-5/profession-cyber-security-needs-know-dan-shoemaker-anne-kohnke-ken-

sigler?context=ubx&refId=8c06ec71-eeab-435e-a590-5db5e9762c7c

De Zan, T. (2019a). *Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions*. Retrieved from https://gcsec.org/wp-content/uploads/2019/02/cyber-ebook-definitivo.pdf

De Zan, T. (2019b). *The Italian Cyber Security Skills Shortage in the International Context*. Retrieved from https://gcsec.org/wp-content/uploads/2019/05/casoIta-ebookENG.PDF

De Zan, T. (2021). Future research on the cyber security skills shortage. In G. Austin (Ed.), *Cyber Security Education: Principles and Policies* (pp. 194–207). Retrieved from https://www.routledge.com/Cyber-Security-Education-Principles-and-Policies/Austin/p/book/9780367421915#

De Zan, T., & Di Franco, F. (2019). *Cybersecurity skills development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database*. https://doi.org/10.2824/525144

De Zan, T., & Yamin, M. M. (2021). *Towards a common ECSC Roadmap: Success factors for the implementation of national cyber security competitions*. Retrieved from https://www.enisa.europa.eu/publications/towards-a-common-ecsc-roadmap

Deakin, H., & Wakefield, K. (2014). Skype interviewing: reflections of two PhD researchers. *Qualitative Research*, *14*(5), 603–616. https://doi.org/10.1177/1468794113488126

Delta Risk. (n.d.). Burp Suite Professional for Web Application Security. Retrieved July 20, 2021, from 2020 website: https://deltarisk.com/blog/how-to-use-burp-suite-professional-for-web-application-security-part-one/

Department of Defense. (2007). *Information Assurance*.

Dewey, J. (1913). *Interest and effort in education* (Mifflin and Company, Ed.). Houghton.

DeWitt, J., Osborne, J., Archer, L., Dillon, J., Willis, B., & Wong, B. (2013). Young Children's Aspirations in Science: The unequivocal, the uncertain and the unthinkable. *International Journal of Science Education*, *35*(6), 1037–1063. https://doi.org/10.1080/09500693.2011.608197

Dipartimento della Protezione Civile. (2020). Coronavirus: 219 i casi accertati in Italia. Retrieved April 1, 2020, from http://www.protezionecivile.gov.it/media-comunicazione/comunicati-stampa/-/content-view/view/1215833

Dominioni, S. (2019). *Cybersecurity: l'architettura della difesa italiana*. Retrieved from https://www.ispionline.it/it/pubblicazione/cybersecurity-larchitettura-della-difesa-italiana-24546

Dunn, M. H., & Merkle, L. D. (2018). Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education - SIGCSE '18*, 62–67. https://doi.org/10.1145/3159450.3159462

Dunst, C. J., & Raab, M. (2006). *Influence of child interests on variations in child behavior and functioning.* Ashville: NC: Winterberry.

Eagle, C. (2013). Computer Security Competitions: Expanding Educational Outcomes. *IEEE Security & Privacy*, *11*(4), 69–71. https://doi.org/10.1109/MSP.2013.83

Eccles, J. S., Fredricks, J. A., & Epstein, A. (2015). Understanding Well-Developed Interests and Activity Commitment. In *Interest in Mathematics and Science Learning* (pp. 315–330). https://doi.org/10.3102/978-0-935302-42-4_18

Edelman, P., Holzer, H., Seleznow, E., Van Kleunen, A., & Watson, E. (2011). *State Workforce Policy: Recent Innovations and an Uncertain Future*. Retrieved from https://m.nationalskillscoalition.org/resources/publications/file/NSC_GU_StateWorkforcePolicy_2011-10.pdf

ENISA. (2018). *ENISA Threat Landscape Report*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport

ENISA. (2019). *ECSC2019*. Retrieved from https://www.europeancybersecuritychallenge.eu/#ecsc

ENISA. (2020). European Cyber Security Challenge 2020 - Event Date Change. Retrieved June 9, 2020, from https://www.enisa.europa.eu/news/enisa-news/european-cyber-security-challenge-2020-dates-changed

European Cybercrime Center. (2019). *Internet Organised Crime Threat Assessment*

(IOCTA). The Hague.

Executive Office of the President of the United States. (2009). *The Comprehensive National Cybersecurity Initiative*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf

Fink, R. (1998). Interest, gender, and literacy development in successful dyslexics. In L. Hoffmann, A. Krapp, K. A. Renninger, & J. Baumert (Eds.), *Interest and learning: Proceedings of the Seeon Conference on Interest and Gender* (pp. 402–408).

Flick, U. (2018). *An Introduction to Qualitative Research* (Sixth Edit). Retrieved from https://us.sagepub.com/en-us/nam/an-introduction-to-qualitative-research/book261109#contents

Floridi, L. (2016). Mature Information Societies—a Matter of Expectations. *Philosophy & Technology*, *29*(1), 1–4. https://doi.org/10.1007/s13347-016-0214-6

Fraser, B. J. (1981). *Test of Science Related Attitude: Handbook*. Retrieved from http://stelar.edc.org/instruments/test-science-related-attitudes-tosra

Frontier economics. (2018). *The impact of artificial intelligence on work*. Retrieved from https://royalsociety.org/-/media/policy/projects/ai-and-work/frontier-review-the-impact-of-AI-on-work.pdf

Fulton, S., Schweitzer, D., & Dressler, J. (2012). What are we teaching in cyber competitions? *2012 Frontiers in Education Conference Proceedings*, 1–5. https://doi.org/10.1109/FIE.2012.6462480

Furchtgott-Roth, D., Jacobson, L., & Mokher, C. (2009). *Strengthening Community College's Influence on Economic Mobility*. Retrieved from https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pcs_assets/2009/pewempcommunitycollegespdf.pdf

Gagliardi, F., Hankin, C., Gal-Ezer, J., McGettrick, A., & Meitern, M. (2016). *Advancing Cybersecurity Research and Education in Europe - Major Drivers of Growth in the Digital Landscape*. Europe Policy Committee Association for Computing Machinery.

Garcia-van Hoogstraten, C., & Bate, L. (2019). *White Paper: Task Force on Cybersecurity Professional Training and Development*. Retrieved from https://cybilportal.org/publications/gfce-white-paper-task-force-on-cybersecurity-

professional-training-and-development/

Garcia, S. M., Tor, A., & Schiff, T. M. (2013). The Psychology of Competition. *Perspectives on Psychological Science*, *8*(6), 634–650. https://doi.org/10.1177/1745691613504114

Gati, I., Krausz, M., & Osipow, S. H. (1996). A taxonomy of difficulties in career decision making. *Journal of Counseling Psychology*, *43*(4), 510–526. https://doi.org/10.1037/0022-0167.43.4.510

GCHQ. (n.d.). GitHub - gchq/CyberChef: The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis. Retrieved July 20, 2021, from https://github.com/gchq/CyberChef

Gibbs, G. (2007). Thematic Coding and Categorizing. In *Analyzing Qualitative Data* (pp. 38–55). https://doi.org/10.4135/9781849208574.n4

Gigova, R. (2017). Who Putin thinks will rule the world - CNN. Retrieved October 28, 2021, from CNN website: https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html

Gokuladas, V. K. (2010). Factors that influence first-career choice of undergraduate engineers in software services companies. *Career Development International*, *15*(2), 144–165. https://doi.org/10.1108/13620431011040941

Goldin, C., & Katz, L. (2007). *The Race between Education and Technology: The Evolution of U.S. Educational Wage Differentials, 1890 to 2005*. https://doi.org/10.3386/w12984

Gottlieb, J., Oudeyer, P.-Y., Lopes, M., & Baranes, A. (2013). Information-seeking, curiosity, and attention: computational and neural mechanisms. *Trends in Cognitive Sciences*, *17*(11), 585–593. https://doi.org/10.1016/j.tics.2013.09.001

Hackett, G., & Betz, N. E. (1981). A self-efficacy approach to the career development of women. *Journal of Vocational Behavior*, *18*(3). https://doi.org/10.1016/0001-8791(81)90019-1

Hagay, G., & Baram-Tsabari, A. (2011). A Shadow Curriculum: Incorporating Students' Interests into the Formal Biology Curriculum. *Research in Science Education*, *41*(5), 611–634. https://doi.org/10.1007/s11165-010-9182-5

Harackiewicz, J. M., Durik, A. M., Barron, K. E., Linnenbrink-Garcia, L., & Tauer, J. M. (2008). The role of achievement goals in the development of interest: Reciprocal relations between achievement goals, interest, and performance. *Journal of Educational Psychology*, *100*(1), 105–122. https://doi.org/10.1037/0022-0663.100.1.105

Henriksen, E. K., Dillon, J., & Ryder, J. (Eds.). (2015). *Understanding Student Participation and Choice in Science and Technology Education*. https://doi.org/10.1007/978-94-007-7793-4

Hidi, S., Weiss, J., Berndorff, D., & Nolan, J. (1998). The role of gender, instruction and a cooperative learning technique in science education across formal and informal settings. In K. A. L. Hoffmann, A. Krapp & J. B. Renninger (Eds.), *Interest and learning: Proceedings of the Seeon conference on interest and gender* (pp. 215–227).

Hidi, S. E., & Renninger, K. A. (2020). On educating, curiosity, and interest development. *Current Opinion in Behavioral Sciences*, *35*, 99–103. https://doi.org/10.1016/j.cobeha.2020.08.002

Hidi, S., & Renninger, K. A. (2006). The Four-Phase Model of Interest Development. *Educational Psychologist*, *41*(2), 111–127. https://doi.org/10.1207/s15326985ep4102_4

HM Government. (2016). *National Cyber Security Strategy 2016-2021*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

HM Government. (2018a). *Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767515/Cyber_security_skills_strategy_211218.pdf

HM Government. (2018b). Search to find Cyber Security experts of the future - GOV.UK. Retrieved November 26, 2019, from https://www.gov.uk/government/news/search-to-find-cyber-security-experts-of-the-future

HM Government. (2019). New online challenge will test teenagers' cyber security skills - GOV.UK. Retrieved November 21, 2019, from

https://www.gov.uk/government/news/new-online-challenge-will-test-teenagers-cyber-security-skills

Hoffman, L. J., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a National Cybersecurity Exercise for Universities. *IEEE Security and Privacy Magazine*, *3*(5), 27–33. https://doi.org/10.1109/MSP.2005.120

Hoi Wai, J. C., LaFleur, M., & Rashid, H. (2019). Data Economy: Radical transformation or dystopia? In *Frontier Technology Quarterly*.

Holland, J. L. (1997). *Making vocational choices: A theory of vocational personalities and work environments*. Psychological Assessment Resources.

Hollenbeck, K. (2008). *Is There a Role for Public Support of Incumbent Worker Training Programs?* Retrieved from https://research.upjohn.org/cgi/viewcontent.cgi?article=1000&context=up_policypapers

Holzer, H. (2013). *Skill Mismatches in Contemporary Labor Markets: How Real? And What Remedies?* Retrieved from http://umdcipe.org/conferences/WorkforceDevelopment/Papers/Workforce_Development_Holzer_Skill_Mismatches_in_Contemporary_Labor_Markets.pdf

Hughes, D., Mann, A., Barnes, S.-A., Baldauf, B., & Rachael, M. (2016). *Careers education: International literature review*. Retrieved from https://www.educationandemployers.org/wp-content/uploads/2016/07/Careers-review.pdf

Hulleman, C. S., & Harackiewicz, J. M. (2009). Promoting Interest and Performance in High School Science Classes. *Science*, *326*(5958), 1410–1412. https://doi.org/10.1126/science.1177067

ICPC. (2020). ICPC Fact Sheet. Retrieved from https://icpc.global/worldfinals/pdf/Factsheet.pdf

ICPC. (2021). The ICPC International Collegiate Programming Contest. Retrieved August 10, 2021, from https://icpc.global/

Il Sole 24 Ore. (n.d.). Exprivia - Ultime notizie su Exprivia - Argomenti del Sole 24 Ore. Retrieved July 20, 2021, from https://argomenti.ilsole24ore.com/exprivia.html

ISACA. (2015). *2015 Global Cybersecurity Status Report*. Retrieved from https://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf

ISACA. (2020). *State of Cybersecurity 2020: Global Update on Workforce Efforts and Resources*. Retrieved from https://www.isaca.org/go/state-of-cybersecurity-2020

ISACA. (2021). *State of Cybersecurity 2021 (Part 1): Global Update on Workforce Efforts, Resources and Budgets*. Retrieved from https://securitydelta.nl/media/com_hsd/report/424/document/state-of-cybersecurity-2021-part-1.pdf

Jackson, K., & Bazeley, P. (2019). Coding foundations. In *Qualitative Data Analysis with NVivo*. London: SAGE Publications Ltd.

James, K. (2008). *Career Academies: Long-Term Impacts on Labor Market Outcomes, Educational Attainment, and Transitions to Adulthood*. Retrieved from https://www.mdrc.org/sites/default/files/full_50.pdf

James Relly, S., & Holmes, C. (2012). *Developing Vocational Excellence: Learning Environments within Work Environments*. Retrieved from https://www.worldskillsuk.org/wp-content/uploads/2020/10/Developing-Vocational-Excellence.pdf

James Relly, S., & Keep, E. (2019). Recognizing and Developing Vocational Excellence Through Skills Competitions. In *Handbook of Vocational Education and Training* (pp. 1–13). https://doi.org/10.1007/978-3-319-49789-1_112-1

James, W. (1890). *The principles of psychology, Vol I.* https://doi.org/10.1037/10538-000

Jarvis, D. (2020). The AI Talent Shortage Isn't Over Yet. Retrieved October 28, 2021, from Wall Streer Journal website: https://deloitte.wsj.com/articles/the-ai-talent-shortage-isnt-over-yet-01602874929

Johnson, K. E., Alexander, J. M., Spencer, S., Leibham, M. E., & Neitzel, C. (2004). Factors associated with the early emergence of intense interests within conceptual domains. *Cognitive Development*, *19*(3), 325–343. https://doi.org/10.1016/j.cogdev.2004.03.001

Jones, L., Palumbo, D., & Brown, D. (2021). Coronavirus: How the pandemic has

changed the world economy - BBC News. Retrieved October 13, 2021, from https://www.bbc.co.uk/news/business-51706225

Kaspersky Lab. (2016a). *LACK OF SECURITY TALENT: AN UNEXPECTED THREAT TO CORPORATE CYBERSAFETY*. Retrieved from https://www.kaspersky.com/blog/security_risks_report_lack_of_security_talent/

Kaspersky Lab. (2016b). *THE CYBERSECURITY SKILLS GAP: A TICKING TIME BOMB*. Retrieved from https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf

Katz, L. F., & Autor, D. H. (1999). Changes in the wage structure and earnings inequality. In *Handbook of Labor Economics*. https://doi.org/10.1016/S1573-4463(99)03007-2

Keep, E. (2006). Market Failure in Skills. *SSDA Catalyst*, (1). Retrieved from https://www.researchonline.org.uk/sds/search/download.do;jsessionid=5A30E0612A636657FF1C84177B85B5ED?ref=B62

Keep, E. (2017). *Current Challenges: Policy Lessons and Implications* (J. Buchanan, D. Finegold, K. Mayhew, & C. Warhurst, Eds.). https://doi.org/10.1093/oxfordhb/9780199655366.013.32

Keep, E., & Mayhew, K. (1988). THE ASSESSMENT: EDUCATION, TRAINING AND ECONOMIC PERFORMANCE. *Oxford Review of Economic Policy*, *4*(3), i–xv. Retrieved from http://www.jstor.org/stable/23606206

Kier, M. W., Blanchard, M. R., Osborne, J. W., & Albert, J. L. (2014). The Development of the STEM Career Interest Survey (STEM-CIS). *Research in Science Education*, *44*(3), 461–481. https://doi.org/10.1007/s11165-013-9389-3

Kohn, A. (1986). *No contest: The case against competition.* Retrieved from https://psycnet.apa.org/record/1986-98204-000

Krapp, A. (2002). An educational-psychological theory of interest and its relation to SDT. In E. L. Deci & R. M. Ryan (Eds.), *Handbook of self-determination research* (pp. 405–427). University of Rochester Press.

Krapp, A. (2007). An educational–psychological conceptualisation of interest. *International Journal for Educational and Vocational Guidance*, *7*(1), 5–21.

https://doi.org/10.1007/s10775-007-9113-9

Krapp, A., & Prenzel, M. (2011). Research on Interest in Science: Theories, methods, and findings. *International Journal of Science Education*, *33*(1), 27–50. https://doi.org/10.1080/09500693.2010.518645

Krutz, D. E., & Richards, T. (2017). Cyber security education. *ACM Inroads*, *8*(4), 5–5. https://doi.org/10.1145/3132217

Kvale, S. (2007a). Analyzing Interviews. In *Doing Interviews* (pp. 102–119). https://doi.org/10.4135/9781849208963.n9

Kvale, S. (2007b). *Doing Interviews*. https://doi.org/10.4135/9781849208963

Lee, W., Lee, M.-J., & Bong, M. (2014). Testing interest and self-efficacy as predictors of academic self-regulation and achievement. *Contemporary Educational Psychology*, *39*(2), 86–99. https://doi.org/10.1016/j.cedpsych.2014.02.002

Lent, R. W., & Brown, S. D. (2019). Social cognitive career theory at 25: Empirical status of the interest, choice, and performance models. *Journal of Vocational Behavior*, *115*, 103316. https://doi.org/10.1016/j.jvb.2019.06.004

Lent, R. W., Brown, S. D., & Hackett, G. (1994). Toward a Unifying Social Cognitive Theory of Career and Academic Interest, Choice, and Performance. *Journal of Vocational Behavior*, *45*(1), 79–122. https://doi.org/10.1006/jvbe.1994.1027

Lent, R. W., Sheu, H.-B., Miller, M. J., Cusick, M. E., Penn, L. T., & Truong, N. N. (2018). Predictors of science, technology, engineering, and mathematics choice options: A meta-analytic path analysis of the social–cognitive choice model by gender and race/ethnicity. *Journal of Counseling Psychology*, *65*(1), 17–35. https://doi.org/10.1037/cou0000243

Lerman, R. (2010). Rediscovering Apprenticeship. In E. Smith & F. Rauner (Eds.), *Rediscovering Apprenticeship: Research Findings of the International Network on Innovative Apprenticeship (INAP)*. https://doi.org/10.1007/978-90-481-3116-7

Leune, K., & Petrilli, S. J. (2017). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. *Proceedings of the 18th Annual Conference on Information Technology Education*, 47–52. https://doi.org/10.1145/3125659.3125686

Li, X., Hou, Z.-J., & Jia, Y. (2015). The influence of social comparison on career decision-making: Vocational identity as a moderator and regret as a mediator. *Journal of Vocational Behavior*, *86*, 10–19. https://doi.org/10.1016/j.jvb.2014.10.003

Lippke, S. (2017). Outcome Expectation. In *Encyclopedia of Personality and Individual Differences* (pp. 1–2). https://doi.org/10.1007/978-3-319-28099-8_1145-1

Lo Iacono, V., Symonds, P., & Brown, D. H. K. (2016). Skype as a Tool for Qualitative Research Interviews. *Sociological Research Online*, *21*(2), 1–15. https://doi.org/10.5153/sro.3952

Long, J. R., & Murphy, P. K. (2005). Connecting through the content: The responsiveness of teacher and student interest in a required course.ù. In T. Flowerday (Ed.), *New directions in the study of interest and engagement*. Symposium conducted at the meeting of the American Educational Research Association. Montreal, Canada.

Maguire, S. (2010). *Tuning In To Local Labor Markets: Findings from the Sectoral Employment Impact Study*. Retrieved from https://ppv.issuelab.org/resources/5101/5101.pdf

Malan, J., Lale-Demoz, E., & Rampton, J. (2018). *Identifying the Role of Further and Higher Education in Cyber Security Skills Development*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767425/The_role_of_FE_and_HE_in_cyber_security_skills_development.pdf

Malterud, K. (2001). Qualitative research: Standards, challenges, and guidelines. *Lancet*, Vol. 358. https://doi.org/10.1016/S0140-6736(01)05627-6

Mason, J. (1996). *Qualitative researching*. London: SAGE Publications Ltd.

Maxwell, J. A. (2012). The Importance of Qualitative Research for Causal Explanation in Education. *Qualitative Inquiry*, *18*(8), 655–661. https://doi.org/10.1177/1077800412452856

Mayhew, K., & Keep, E. (2014). *Industrial strategy and the future of skills policy: The high road to sustainable growth*. Retrieved from https://www.cipd.co.uk/Images/industrial-strategy-and-the-future-of-skills-

policy_2014_tcm18-10247.pdf

Mayhew, K., Relly, S. J., Chankseliani, M., & Laczik, A. (2013). *Benefits of Developing Vocational Excellence: A Report to the National Apprenticeship Service of Project 3 of the DUVE suite of projects*. Retrieved from http://vocationalexcellence.education.ox.ac.uk/wordpress/wp-content/uploads/2014/02/DUVE-Project-3-Final-Report-Phase-1.pdf

McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the Flag as Cyber Security Introduction. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5479–5486. https://doi.org/10.1109/HICSS.2016.677

McDaniel, M. A., Waddill, P. J., Finstad, K., & Bourg, T. (2000). The effects of text-based interest on attention and recall. *Journal of Educational Psychology*, *92*(3), 492–502. https://doi.org/10.1037/0022-0663.92.3.492

McDonald, V. L. (2010). Before-and-After Case Study Design. In A. Mills, G. Durepos, & E. Wiebe (Eds.), *Encyclopedia of Case Study Research*. https://doi.org/10.4135/9781412957397

McGuinness, S., Pouliakas, K., & Redmond, P. (2018). Skills Mismatch: Concepts, Measurement and Policy Approaches. *Journal of Economic Surveys*, *32*(4), 985–1015. https://doi.org/10.1111/joes.12254

McHenry, D., Borges, T., Bollen, A., Shah, J. N., Donaldson, S., Crozier, D., & Furnell, S. (2021). *Cyber security skills in the UK labour market 2021*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973802/Ipsos_MORI_Cyber_Skills_in_the_UK_2021_v1.pdf

Melchior, A., Burack, C., Hoover, M., & Haque, Z. (2018). *FIRST Longitudinal Study: Findings at 48 Month Follow-Up (Year 5 Report)*. Retrieved from https://www.firstinspires.org/sites/default/files/uploads/resource_library/impact/first-longitudinal-study-summary-year-5.pdf

Meyer, D. K., & Turner, J. C. (2002). Discovering Emotion in Classroom Motivation Research. *Educational Psychologist*, *37*(2), 107–114. https://doi.org/10.1207/S15326985EP3702_5

Michaelis, J., & Nathan, M. (2015). The Four-Phase Interest Development in

Engineering Survey. *ASEE Annual Conference and Exposition Proceedings*. https://doi.org/10.18260/p.25117

Migration Advisory Committee. (2019). *Full review of the Shortage Occupation List*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/806331/28_05_2019_Full_Review_SOL_Final_Report_1159.pdf

Miller, K., Sonnert, G., & Sadler, P. (2018). The influence of students' participation in STEM competitions on their interest in STEM careers. *International Journal of Science Education, Part B*, *8*(2), 95–114. https://doi.org/10.1080/21548455.2017.1397298

Ministero dell'Istruzione. (2021a). *Focus "Principali dati della scuola – Avvio Anno Scolastico 2021/2022."* Retrieved from https://miur.gov.it/documents/20182/0/Principali+dati+della+scuola+-+Focus+avvio+anno+scolastico+2021-2022.pdf/6d54b1ed-4c08-bea3-2d13-db241030e3f0?version=1.1&t=1633623787269

Ministero dell'Istruzione. (2021b). Scuola secondaria di secondo grado. Retrieved December 7, 2021, from https://www.miur.gov.it/scuola-secondaria-di-secondo-grado

Ministry of Economy Trade and Industry. (2016). *IT人材の最新動向と将来推計に関する調査結果*. Retrieved from https://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf

Minnaert, A., Boekaerts, M., & De Brabander, C. (2007). Autonomy, Competence, and Social Relatedness in Task Interest within Project-Based Education. *Psychological Reports*, *101*(2), 574–586. https://doi.org/10.2466/pr0.101.2.574-586

Mitchell, M. (1993). Situational interest: Its multifaceted structure in the secondary school mathematics classroom. *Journal of Educational Psychology*, *85*(3), 424–436. https://doi.org/10.1037/0022-0663.85.3.424

Morrow, J. J., Mood, D., Disch, J., & Kang, M. (2016). *Measurement and Evaluation in Human Performance With Web Study Guide* (5th ed.). Human Kinetics.

Mullins, B. E., Lacey, T. H., Mills, R. F., Trechter, J. E., & Bass, S. D. (2007). How the

Cyber Defense Exercise Shaped an Information-Assurance Curriculum. *IEEE Security & Privacy Magazine*, *5*(5), 40–49. https://doi.org/10.1109/MSP.2007.111

Nachreiner, C. (2019). Can CTFs Help Close The Cybersecurity Skills Gap? Retrieved December 5, 2019, from Council Post website: https://www.forbes.com/sites/forbestechcouncil/2019/11/22/can-ctfs-help-close-the-cybersecurity-skills-gap/#15607ed512b0

National Cyber Security Centre. (2017). Penetration Testing - NCSC.GOV.UK. Retrieved February 4, 2021, from https://www.ncsc.gov.uk/guidance/penetration-testing

National Research Council. (2011). *Successful K-12 STEM Education: Identifying Effective Approaches in Science, Technology, Engineering, and Mathematics*. https://doi.org/10.17226/13158

Nevo, D. (2006). Evaluation in Education. In I. Shaw, J. Greene, & M. Mark (Eds.), *The SAGE Handbook of Evaluation* (pp. 442–460). https://doi.org/10.4135/9781848608078

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

NIST. (2018). *Cybersecurity Competitions*. Retrieved from https://www.nist.gov/system/files/documents/2018/09/24/cybersecurity_competitions.pdf

Nokelainen, P., Pylväs, L., & Rintala, H. (2019). Skills Competitions for Promoting Vocational Excellence. In *Handbook of Vocational Education and Training* (pp. 1239–1250). https://doi.org/10.1007/978-3-319-94532-3_69

Nokelainen, P., & Stasz, C. (2016). *What contributes to vocational excellence? A study of the characteristics of WorldSkills UK participants for WorldSkills*. Retrieved from http://vocationalexcellence.education.ox.ac.uk/wordpress/wp-content/uploads/2016/05/Project-1-Final-What-contributes-to-Vocational-Excellence.pdf

Nolen, S. B. (2007). Young Children's Motivation to Read and Write: Development in Social Contexts. *Cognition and Instruction*, *25*(2–3), 219–270.

https://doi.org/10.1080/07370000701301174

Nurse, J. R. C., Grammatopoulos, A., Adamos, K., & Di Franco, F. (2021). *Addressing the EU cyber security skills shortage and gap through higher education*. Retrieved from https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

OECD. (2017). *Getting Skills Right: Good Practice in Adapting to Changing Skill Needs*. https://doi.org/10.1787/9789264277892-en

Oltsik, J. (2017). *The Life and Times of Cybersecurity Professionals*. Retrieved from https://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Nov-2017.pdf

Oltsik, J. (2021). *The Life and Times of Cybersecurity Professionals 2021*. Retrieved from https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

Oltsik, J., & Lundell, B. (2021). *The Life and Times of Cybersecurity Professionals 2021 - Volume V*. ESG-ISSA.

Organization of American States. (2020). *Cybersecurity education: Planning for the Future Through Workforce Development*. Retrieved from http://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf

Owen, K., Dubourg, R., Johnson, D., Allen, C., Black, C., Chapman, B., … Weatherburn, M. (2011). *The Magenta Book: Guidance for evaluation*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/220542/magenta_book_combined.pdf

Ozturk, M. A., & Debelak, C. (2008). Affective Benefits from Academic Competitions for Middle School Gifted Students. *Gifted Child Today*, *31*(2), 48–53. https://doi.org/10.4219/gct-2008-758

Palmer, D. (2004). RESEARCH REPORT. *International Journal of Science Education*, *26*(7), 895–908. https://doi.org/10.1080/0950069032000177262

Palmer, D. H. (2009). Student interest generated during an inquiry skills lesson. *Journal of Research in Science Teaching*, *46*(2), 147–165.

https://doi.org/10.1002/tea.20263

Patall, E. A., & Hooper, S. Y. (2019). The Promise and Peril of Choosing for Motivation and Learning. In *The Cambridge Handbook of Motivation and Learning* (pp. 238–262). https://doi.org/10.1017/9781316823279.012

Pedley, D., Borges, T., Bollen, A., Shah, J. N., Donaldson, S., Furnell, S., & Crozier, D. (2020). *Cyber security skills in the UK labour market 2020*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/959164/Cyber_security_skills_report_in_the_UK_labour_market_2020_V2.pdf

Pedley, D., McHenry, D., Motha, H., & Navin, J. S. (2018). *Understanding the UK cyber security skills labour market - Research report for the Department for Digital, Culture, Media and Sport*. Retrieved from https://www.ipsos.com/sites/default/files/ct/publication/documents/2019-01/understanding_the_uk_cyber_security_skills_labour_market.pdf

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. *IEEE Security Privacy*, *18*(2), 68–74. https://doi.org/10.1109/MSEC.2020.2969409

Petropoulos, G. (2021). *Automation, Covid-19 and labour markets*. Retrieved from https://www.adb.org/sites/default/files/publication/688896/adbi-wp1229.pdf

Polk, T. (2016). Building the Workforce through Cybersecurity Competitions. Retrieved from the White House, President Barack Obama website: https://obamawhitehouse.archives.gov/blog/2016/07/27/building-workforce-through-cybersecurity-competitions

Ponemon Institute, & Accenture. (2019). *The Cost of Cybercrime*. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Porro, G. (2019). L'Italia è arrivata seconda all'European Cybersecurity Challenge - Wired. Retrieved October 22, 2019, from https://www.wired.it/internet/web/2019/10/14/italia-cyberdefence-european-cybersecurity-challenge/?refresh_ce=

Presidenza del Consiglio dei Ministri. (2018). *Relazione sulla politica dell'informatione per la sicurezza*. Rome.

Pusey, P., Gondree, M., & Peterson, Z. (2016). The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations. *IEEE Security & Privacy*, *14*(6), 90–95. https://doi.org/10.1109/MSP.2016.119

Pye Tait Consulting, & Carol Stanfield Consulting. (2021). *International approaches to careers interventions*. Retrieved from https://files.eric.ed.gov/fulltext/ED612488.pdf

Ra, S., Shrestha, U., Khatiwada, S., Yoon, S. W., & Kwon, K. (2019). The rise of technology and impact on skills. *International Journal of Training Research*, *17*(sup1), 26–40. https://doi.org/10.1080/14480220.2019.1629727

Radunović, V., & Rüfenacht, D. (2016). *Cyber Security Competence Building Trend*. Retrieved from https://www.diplomacy.edu/sites/default/files/Cybersecurity Full Report.pdf

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the Cyber Security Body of Knowledge. *IEEE Security & Privacy*, *16*(3), 96–102. https://doi.org/10.1109/MSP.2018.2701150

Relly, S. J. (2016). *Developing & Understanding Vocational Excellence: Final Report*. Retrieved from http://vocationalexcellence.education.ox.ac.uk/wordpress/wp-content/uploads/2016/03/DuVE-project-Final-report.pdf

Renninger, K. Ann, Bachrach, J. E., & Hidi, S. E. (2019). Triggering and maintaining interest in early phases of interest development. *Learning, Culture and Social Interaction*, *23*, 100260. https://doi.org/10.1016/j.lcsi.2018.11.007

Renninger, K. Ann, & Hidi, S. (2011). Revisiting the Conceptualization, Measurement, and Generation of Interest. *Educational Psychologist*, *46*(3), 168–184. https://doi.org/10.1080/00461520.2011.587723

Renninger, K. Ann, & Hidi, S. (2016). *The Power of Interest for Motivation and Engagement*. Retrieved from https://www.routledge.com/The-Power-of-Interest-for-Motivation-and-Engagement/Renninger-Hidi/p/book/9781138779792#

Renninger, K. Ann, & Hidi, S. E. (2020). To Level the Playing Field, Develop Interest. *Policy Insights from the Behavioral and Brain Sciences*, *7*(1), 10–18.

https://doi.org/10.1177/2372732219864705

Renninger, K. Ann, & Schofield, L. S. (2014). *Assessing STEM interest as a developmental motivational variable.* American Educational Research Association.

Renninger, K. Ann, & Su, S. (2019). Interest and Its Development, Revisited. In R. M. Ryan (Ed.), *The Oxford Handbook of Human Motivation* (pp. 203–226). https://doi.org/10.1093/oxfordhb/9780190666453.013.12

Renninger, K.A, Ewen, L., & Lasher, A. . (2002). Individual interest as context in expository text and mathematical word problems. *Learning and Instruction*, *12*(4), 467–490. https://doi.org/10.1016/S0959-4752(01)00012-3

Ricci, M., & Jessica, G. (2017). Cybersecurity Games: Building Tomorrow's Workforce. *Journal of Law & Cyber Warfare*, *5*(2), 183–224. Retrieved from https://www.jstor.org/stable/26441274

Roder, A., & Elliott, M. (2011). *A Promising Start Year Up's Initial Impacts on Low-Income Young Adults' Careers*. Retrieved from https://www.issuelab.org/resources/25551/25551.pdf

Rottinghaus, P. J., Larson, L. M., & Borgen, F. H. (2003). The relation of self-efficacy and interests: a meta-analysis of 60 samples. *Journal of Vocational Behavior*, *62*(2), 221–236. https://doi.org/10.1016/S0001-8791(02)00039-8

RSM. (2020a). *Evaluation of CNI Apprenticeships Programme*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1009062/Evaluation_of_CNI_Apprenticeships_Programme_.pdf

RSM. (2020b). *Evaluation of cyber critical national infrastructure apprenticenships programme and other interventions in this space - final report*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1009062/Evaluation_of_CNI_Apprenticeships_Programme_.pdf

RSM. (2020c). *Evaluation of the Cyber Security Postgraduate Bursaries Scheme*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1009065/Evaluation_of_DCMS_Cyber_Security_Postgraduate_Bursaries_Scheme.pdf

RSM. (2020d). *Evaluation of the Cyber Skills Immediate Impact Fund Pilot*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1009064/Evaluation_of_Cyber_Skills_Immediate_Impact_Fund_Pilot.pdf

Russon, M.-A., & Hooker, L. (2021). UK “heading towards digital skills shortage disaster” - BBC News. Retrieved October 28, 2021, from BBC website: https://www.bbc.co.uk/news/business-56479304

Saka, N., Gati, I., & Kelly, K. R. (2008). Emotional and Personality-Related Aspects of Career-Decision-Making Difficulties. *Journal of Career Assessment*, *16*(4), 403–424. https://doi.org/10.1177/1069072708318900

Sansone, C., Thoman, D., & Fraughton, T. (2015). The relation between interest and self-regulation in mathematics and science. In & S. H. K. A. Renninger, M. Nieswandt (Ed.), *Interest in mathematics and science learning*. Washington, D.C.: American Educational Research Association.

Sansone, C., Weir, C., Harpster, L., & Morgan, C. (1992). Once a boring task always a boring task? Interest as a self-regulatory mechanism. *Journal of Personality and Social Psychology*, *63*(3), 379–390. https://doi.org/10.1037/0022-3514.63.3.379

Sarrocco, C. (2002). *Elements and principles of the information society*. Retrieved from http://www.itu.int/osg/spu/wsis-themes/access/BackgroundPaper/IS Principles.pdf

Savino, P. (2020). Punteggi test Medicina: analisi per scegliere le preferenze. Retrieved March 17, 2021, from https://www.ammissione.it/area-sanitaria/analisi-punteggi-test-medicina/17502/

Schaufeli, W. B., Bakker, A. B., & Salanova, M. (2006). The Measurement of Work Engagement With a Short Questionnaire: A Cross-National Study. *Educational and Psychological Measurement*, *66*(4), 701–716. https://doi.org/10.1177/0013164405282471

Schermer, J. A. (2016). Vocational Interests. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of Personality and Individual Differences* (pp. 1–2). https://doi.org/10.1007/978-3-319-28099-8_801-1

Schleicher, A. (2021). What will education look like in 20 years? Retrieved October 29, 2021, from World Economic Forum website: https://www.weforum.org/agenda/2021/01/future-of-education-4-scenarios/

Schmidt, H. G., & Rotgans, J. I. (2021). Epistemic Curiosity and Situational Interest: Distant Cousins or Identical Twins? *Educational Psychology Review*, *33*(1), 325–352. https://doi.org/10.1007/s10648-020-09539-9

Schneider, F. B. (2013). Cybersecurity Education in Universities. *IEEE Security & Privacy*, *11*(4), 3–4. https://doi.org/10.1109/MSP.2013.84

Sheu, H.-B., Lent, R. W., Brown, S. D., Miller, M. J., Hennessy, K. D., & Duffy, R. D. (2010). Testing the choice model of social cognitive career theory across Holland themes: A meta-analytic path analysis. *Journal of Vocational Behavior*, *76*(2), 252–264. https://doi.org/10.1016/j.jvb.2009.10.015

Shires, J. (2020). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*, *41*(1), 82–107. https://doi.org/10.1080/13523260.2019.1670006

Shretta, R. (2020). The economic impact of COVID-19. Retrieved October 13, 2021, from Research\ University of Oxford website: https://www.research.ox.ac.uk/article/2020-04-07-the-economic-impact-of-covid-19

Silverman, D. (2015). Data Analysis. In *Interpreting Qualitative Data* (pp. 145–179).

Silvia, P. J. (2006). *Exploring the Psychology of Interest*. https://doi.org/10.1093/acprof:oso/9780195158557.001.0001

Smith, B. (2021). America faces a cybersecurity skills crisis: Microsoft launches national campaign to help community colleges expand the cybersecurity workforce. Retrieved November 5, 2021, from Official Microsoft Blog website: https://blogs.microsoft.com/blog/2021/10/28/america-faces-a-cybersecurity-skills-crisis-microsoft-launches-national-campaign-to-help-community-colleges-expand-the-cybersecurity-workforce/

Spencer, L., Ritchie, J., O'Connor, W., Garreth, M., & Ormston, R. (2014). Analysis in practice. In K. Jackson, J. Ritchie, C. M. Nicholls, & R. Ormston (Eds.), *Qualitative Research Practice: A Guide for Social Science Students and Researchers* (Second). Retrieved from https://us.sagepub.com/en-us/nam/qualitative-research-

practice/book237434

Stanne, M. B., Johnson, D. W., & Johnson, R. T. (1999). Does competition enhance or inhibit motor performance: A meta-analysis. *Psychological Bulletin*, *125*(1), 133–154. https://doi.org/10.1037/0033-2909.125.1.133

Stoltenberg, J. (2019). NATO will defend itself. Retrieved December 18, 2019, from Prospect website: https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

Strauss, A. L. (1987). *Qualitative Analysis for Social Scientists*. Cambridge: Cambridge University Press.

Taddeo, M. (2019). Is Cybersecurity a Public Good? *Minds and Machines*, *29*(3), 349–354. https://doi.org/10.1007/s11023-019-09507-5

Taddeo, M., & Floridi, L. (2018a). How AI can be a force for good. *Science*, *361*(6404), 751–752. https://doi.org/10.1126/science.aat5991

Taddeo, M., & Floridi, L. (2018b). Regulate artificial intelligence to avert cyber arms race. *Nature*, *556*(7701), 296–298. https://doi.org/10.1038/d41586-018-04602-6

Telsy. (n.d.). Telsy – Innovation for security. Retrieved July 20, 2021, from https://www.telsy.com/

The Council of Economic Advisers. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy*. Retrieved from https://www.hsdl.org/?view&did=808776

The Joint Committee on the National Security Strategy. (2018). *Cyber Security Skills and the UK's Critical National Infrastructure: Government Response to the Committee's Second Report of Session 2017–19*. Retrieved from https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1658/1658.pdf

The Secretary of Commerce and the Secretary of Homeland Security. (2017). *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*. Retrieved from https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf

The White House. (2019). Executive Order on America's Cybersecurity Workforce.

Retrieved November 3, 2021, from Executive Order website: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

Timoteo, M., Antonelli, G., Bartolini, E., Binassi, S., Bonafe', E., Bregolin, G., … Tampellini, L. (2021). *XXIII Indagine Profilo dei Laureati 2020*. Retrieved from https://www.almalaurea.it/sites/almalaurea.it/files/docs/universita/profilo/profilo2021/almalaurea_profilo_rapporto2021.pdf

Tobey, D. H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. *ACM Inroads*. https://doi.org/10.1145/2568195.2568213

Trautwein, U., Lüdtke, O., Nagy, N., Lenski, A., Niggli, A., & Schnyder, I. (2015). Using individual interest and conscientiousness to predict academic effort: Additive, synergistic, or compensatory effects? *Journal of Personality and Social Psychology*, *109*(1), 142–162. https://doi.org/10.1037/pspp0000034

Trend Micro. (n.d.). Exploit - Definition. Retrieved May 20, 2021, from https://www.trendmicro.com/vinfo/us/security/definition/exploit

Trend Micro. (2019). LOKI Malware Information. Retrieved August 12, 2020, from https://success.trendmicro.com/solution/1117830-loki-malware-information

Trochim, W. M. K. (2021). Descriptive Statistics - Research Methods Knowledge Base. Retrieved October 4, 2021, from https://conjointly.com/kb/descriptive-statistics/

Turner, G. E., Deemer, E. D., Tims, H., Corbett, K., & Mhire, J. (2014). Cyber Value and Interest Development: Assessment of a STEM Career Intervention for High School Students. *The Electronic Journal of Science Education*, *18*, 1–15.

Tyler-Wood, T., Knezek, G., & Christensen, R. (2010). Instruments for Assessing Interest in STEM Content and Careers. *Journal of Technology and Teacher Education*, *18*(2), 345–368. Retrieved from https://www.learntechlib.org/p/32311

U.S. Bureau of Labor Statistics. (2021). Information Security Analysts: Occupational Outlook Handbook. Retrieved October 12, 2021, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

University of Oslo. (n.d.). *ROSE Questionnaire*. Retrieved from https://roseproject.no/key-documents/key-docs/master-rose-q.doc

University of Phoenix, $(ISC)^2$, & $(ISC)^2$ Foundation. (2014). *Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals*. Retrieved from https://www.nationalcyberwatch.org/ncw-content/uploads/2016/03/cybersecurity-report-1-1.pdf

van den Hurk, A., Meelissen, M., & van Langen, A. (2019). Interventions in education to prevent STEM pipeline leakage. *International Journal of Science Education*, *41*(2), 150–164. https://doi.org/10.1080/09500693.2018.1540897

van Rensburg, A. J., & Baker, R. (2021). *CTF Events: Contemporary Practices and State-of-the-Art in Capture-the-Flag Competitions*. Retrieved from https://www.enisa.europa.eu/publications/ctf-events

Verhoeff, T. (1997). *The role of competitions in education*.

Vinberg, S. (2020). The Cybersecurity Skills Gap: It Doesn't Have to Be This Way. Retrieved October 26, 2021, from https://www.darkreading.com/careers-and-people/the-cybersecurity-skills-gap-it-doesn-t-have-to-be-this-way

Vivaldelli, R. (2021). L'operazione cybersecurity: salta la fondazione di 007 voluta da Conte - ilGiornale.it. Retrieved October 13, 2021, from https://www.ilgiornale.it/news/politica/loperazione-cybersecurity-salta-fondazione-007-voluta-conte-1948083.html

Wang, X. H., & Yang, B. (2003). Why Competition may Discourage Students from Learning? A Behavioral Economic Analysis. *Education Economics*, *11*(2), 117–128. https://doi.org/10.1080/09645290210131656

Wee, C., Bashir, M., & Memon, N. (2016). The Cybersecurity Competition Experience: Perceptions from Cybersecurity Workers. *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. Retrieved from https://www.usenix.org/conference/soups2016/workshop-program/wsiw16/presentation/wee

Weimann, G. (2015). *Terrorism in Cyberspace: The Next Generation*. Retrieved from https://www.wilsoncenter.org/book/terrorism-cyberspace-the-next-generation

Weinhardt, L. S., Galvao, L. W., Yan, A. F., Stevens, P., Mwenyekonde, T. N., Ngui, E., … Watkins, S. C. (2017). Mixed-Method Quasi-Experimental Study of Outcomes of a Large-Scale Multilevel Economic and Food Security Intervention on HIV Vulnerability in Rural Malawi. *AIDS and Behavior*, *21*(3), 712–723. https://doi.org/10.1007/s10461-016-1455-1

Welch, A., & Huffman, D. (2011). The Effect of Robotics Competitions on High School Students' Attitudes Toward Science. *School Science and Mathematics*, *111*(8), 416–424. https://doi.org/10.1111/j.1949-8594.2011.00107.x

Werther, J., Zhivich, M., Leek, T., & Zeldovich, N. (2011). Experiences in Cyber Security Education: The {MIT} Lincoln Laboratory Capture-the-Flag Exercise. *4th Workshop on Cyber Security Experimentation and Test ({CSET} 11)*. Retrieved from https://www.usenix.org/conference/cset11/experiences-cyber-security-education-mit-lincoln-laboratory-capture-flag-exercise

Whiston, S. C., & Noblin James, B. (2012). Promotion of career choice. In S. D. Brown & R. W. Lent (Eds.), *Career Development and Counseling* (2nd ed., pp. 565–595). Retrieved from https://www.wiley.com/en-ca/Career+Development+and+Counseling%3A+Putting+Theory+and+Research+to+Work%2C+2nd+Edition-p-9781118063354

White, H., & Raitzer, D. A. (2017). *Impact Evaluation of Development Interventions: A Practical Guide*. https://doi.org/10.22617/TCS179188-2

Wikipedia. (n.d.). Mr. Robot. Retrieved February 12, 2021, from https://en.wikipedia.org/wiki/Mr._Robot

Williams, H., Kearney, J., Zatterin, G., Donaldson, S., Crozier, D., & Nurse, J. (2021). *Understanding the Cyber Security Recruitment Pool*. Retrieved from https://www.gov.uk/government/publications/understanding-the-cyber-security-recruitment-pool

World Economic Forum. (2019). *The Global Risks Report 2019*. Retrieved from http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

World Health Organization. (2020). Naming the coronavirus disease (COVID-19) and the virus that causes it. Retrieved April 1, 2020, from https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-

guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

World Health Organization. (2021). WHO Coronavirus (COVID-19) Dashboard | WHO Coronavirus (COVID-19) Dashboard With Vaccination Data. Retrieved October 13, 2021, from https://covid19.who.int/

WorldSkills. (2019). Competition. Retrieved August 10, 2021, from https://worldskills2019.com/en/event/competition/index.html

WorldSkills. (2021). WorldSkills Shanghai 2022. Retrieved August 10, 2021, from https://worldskills2022.com/en/event/skills/

Xie, K. (2019). Here's how we can tackle the growing cybersecurity skills gap | World Economic Forum. Retrieved November 1, 2021, from World Economic Forum website: https://www.weforum.org/agenda/2019/01/addressing-the-growing-cybersecurity-skills-gap/

Žáková, G. (2018). Cyberspace: Global Public Goods? *Acta Oeconomica Pragensia*, *2018*(2), 68–82. https://doi.org/10.18267/j.aop.602

Annex I: List of acronyms

AI	Artificial Intelligence
CTF	Capture-the-Flag
CCIT	CyberChallenge.IT
CDT	Centre for Doctoral Training
CEDEFOP	European Centre for the Development of Vocational Training
CG	Control Group
CoS	Confirmation of Status
CSSS	Cyber Security Skills Shortage
CTFs	Capture The Flag competitions
DiD	Difference-in-Difference
DUVE	Developing and Understanding Vocational Excellence
ECSC	European Cyber Security Challenge
ENISA	European Union Network and Information Security Agency
ESG	Enterprise Strategy Group
EU	European Union
FIRST	First Inspiration and Recognition of Science and Technology
GDPR	General Data Protection Regulation
ICT	Information Communication Technology
ISACA	Information Systems Audit and Control Association
ISSA	Information Systems Security Association
IT	Information Technology
ICPC	International Collegiate Programming Contest
NCSSC	National cyber security skills competition
OCCIT	OpenCyberChallenge.IT
OST	Out-of-School Time
SOL	Shortage Occupation List
STEM	Science Technology Engineering and Mathematics
TG	Treatment Group
UK	United Kingdom
US	United States
WEF	World Economic Forum

Annex II: Survey questionnaires

"Before" survey (February 2020)

- *How did you do so far in the CCIT?*
  - I did the pre-test online, but I was not selected for the admission test in February
  - I sat the morning admission test in February, but I was not admitted to the afternoon test
  - I sat the afternoon admission test in February, but I was not selected for the training at the local university
  - I was selected for the training at the local university

- *In which university did you sit the admission test?*
  - List of all attending institutions
  - …
  - …

Background information

- *What is your gender?*
  - Female
  - Male
  - Prefer not to say

- *In which Italian region were you born?*
  - List of all Italian regions
  - …
  - I was not born in Italy

- *Are you a high school or a university student?*
  - High school
  - University

- *What type of high school are you enrolled in?*
  - Liceo
  - Istituto Tecnico
  - Istituto Professionale
  - Other

- *(If selected high school student) What type of Liceo are you enrolled in?*
  - Liceo artistico
  - Liceo classico
  - Liceo linguistico
  - Licei musicale e coreutici
  - Liceo scientifico
  - Liceo scientifico – opzione Scienze applicate
  - Liceo scientifico – sezione a indirizzo sportivo
  - Liceo scienze umane
  - Liceo scienze umane – opzione economico sociale

- *What type of Istituto Tecnico are you enrolled in?*

- Amministrazione, Finanza e Marketing
- Turismo
- Meccanica, Meccatronica ed Energia
- Trasporti e Logistica
- Elettronica ed Elettrotecnica
- Informatica e Telecomunicazioni
- Grafica e Comunicazione
- Chimica, Materiali e Biotecnologie
- Sistema Moda
- Agraria, Agroalimentare e Agroindustria
- Costruzioni, Ambiente e Territorio

- *What type of Istituto Professionale are you enrolled in?*
  - Agricoltura, sviluppo rurale, valorizzazione dei prodotti del territorio e gestione delle risorse forestali e montane
  - Pesca commerciale e produzioni ittiche
  - Industria e artigianato per il Made in Italy
  - Manutenzione e assistenza tecnica
  - Gestione delle acque e risanamento ambientale
  - Servizi commerciali
  - Enogastronomia e ospitalità alberghiera
  - Servizi culturali e dello spettacolo
  - Servizi per la sanità e l'assistenza sociale
  - Arti ausiliarie delle professioni sanitarie

- *What is your current GPA?*
  - Below 6.00
  - Between 6.00 - 7.99
  - Between 8.00 - 9.99

- *(If selected university student) Are you enrolled in a bachelor's or a master's degree?*
  - Bachelor's degree
  - Master's degree

- *In which university department are you currently enrolled in?*
  - Electronics or telecommunications (if you study electronic engineer you must select this option)
  - Computer science (if you study computer science-engineering you must select this option)
  - Engineering
  - Mathematics, statistics or physics
  - Chemistry and biotechnology
  - Medical science or pharmacy
  - Law
  - Social sciences (economics, political science, sociology, psychology, etc.)
  - Classics (history, modern languages or classics, literature, etc)
  - Other

- *What is your current overall GPA?*
  - 18 - 22
  - 23 - 26
  - 27 – 30

- *What is the combined monthly income of your parents?*
  - €0 - €2.500
  - €2.501 - €4.000

- €4.001 - €8.000
- > €8.001
- I do not know

- *Has at least one of your parents ever studied cyber security or IT more broadly in school or at university?*
  - Yes
  - No
  - Do not know

- *Has at least one of your parents ever worked in cyber security or IT more broadly?*
  - Yes
  - No
  - I do not know

- *Have you ever been enrolled, either online or face-to-face, in a cyber security course?*
  - Yes
  - No
  - I do not know

- *How many cyber security competitions have you attended in your life before this year's CyberChallenge.IT?*
  - 0
  - 1-5
  - 6-10

- More than 10

- *How did you learn cyber security?*
  - I currently do not know anything, or I know little, about cyber security
  - By myself
  - Through cyber security competitions
  - My parents taught me
  - In the classroom
  - Due to an internship or other professional experiences
  - Other

- *Select one level of agreement to indicate how you feel about each statement (Strongly disagree, Disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Agree, Strongly agree)*
  - If I had enough time and resources, I would be able to learn new cyber security concepts and skills
  - If I attended a cyber security course/class, I would get good grades
  - I can manage to solve the majority of cyber security issues that I face
  - If I wanted, I would be able to acquire, either by myself or through a degree/certification, cyber security knowledge and skills to become a professional in this sector

- *Have you ever been paid for a cyber security/IT service that you provided and/or have you been previously employed in a cyber security job?*
  - Yes
  - No
  - Do not know

- *What are the two main reasons why you signed up to CyberChallenge.IT 2020?*
  - To understand more about cyber security careers
  - I love challenging myself
  - I love cyber security competitions
  - To increase cyber security knowledge and skills
  - To get to know new people
  - To network with people from the industry
  - I am curious to try it out
  - Other

Interest in cyber security and its careers

- *Select one level of agreement to indicate how you feel about each statement (Strongly disagree, Disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Agree, Strongly agree)*
  - I am interested in cyber security: I would like to learn more about it and develop related skills
  - I would like to have a career in the cyber security sector
  - I would like to pursue a degree and/or a certification that is needed for a career in cybersecurity
  - I would like to use my cyber security knowledge and skills to do interesting things at work
  - My family has encouraged (or would encourage) me to study IT and/or cyber security
  - I would like to have a successful career in cyber security and make a substantial contribution to the sector
  - Cyber security professionals have an important role in the world
  - I would like to talk about cyber security careers with professionals from the same sector
  - A career in cyber security would be fulfilling

- I would like to work with people that make systems, data and networks more secure
- If my application for a cyber security position was rejected, I would apply again to other cyber security jobs
- I already know what kind of jobs and professional opportunities there are in the cyber security sector
- I would like to attend cyber security career fairs and presentations
- I will apply to cyber security jobs when I leave high school/university education

"After" survey (October 2020)

Achievements during the CCIT

- *How did you do so far in the CCIT?*
  - I did the pre-test online, but I was not selected to sit the admission test in February
  - I sat the morning admission test in February, but I was not admitted to the afternoon test
  - I sat the afternoon admission test in February, but I was not selected for the training at the local university
  - I was selected for the training at the local university, but I did not attend it
  - I was selected for the training at the local university and I attended it
  - I was selected to attend the national Cyber Challenge in October

- *Have you participated in the Open CCIT programme?*
  - No

- Yes, but I did not receive the attendance certificate
- Yes, and I received the attendance certificate

Cyber security interest formation

- *How did you become interested in cyber security? Select up to 3 answers*
  - Formal education (either in high school or at university)
  - A professor encouraged me to get deeper in the subject
  - Curiosity (for example reading online or through social media)
  - The CCIT
  - Cyber security competitions
  - TV shows (like for example Mr. Robots)
  - Friends and/or family members
  - I was victim of online crime
  - Reading specialist content
  - I am not interested in cyber security
  - Other

Briefly describe how you have become interested in cyber security …

Cyber security interest

- *Select one level of agreement to indicate how you feel about each statement (Strongly disagree, Disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Agree, Strongly agree)*
  - I am interested in cyber security: I would like to learn more about it and develop skills
  - I would like to have a career in the cyber security sector
  - I would like to pursue a degree and/or a certification that is needed for a career in cybersecurity

- I would like to use my cyber security knowledge and skills to do interesting things at work
- My family has encouraged (or would encourage) me to study IT and/or cyber security
- I would like to have a successful career in cyber security and make a substantial contribution to the sector
- Cyber security professionals have an important role in the world
- I would like to talk about cyber security careers with professionals from the same sector
- A career in cyber security would be fulfilling
- I would like to work with people that make systems, data and networks more secure
- If my application for a cyber security position was rejected, I would apply again to other cyber security jobs
- I already know what kind of jobs and professional opportunities there are in the cyber security sector
- I would like to attend cyber security career fairs and presentations
- I will apply to cyber security jobs when I leave high school/university education

Cyber security and career plans

- *Are you interested in a specific bachelor's/master's degree or other courses?*
  - Yes (*If yes, can you specify?*)
  - Maybe
  - I do not know

- *Are you interested in a specific cyber security role?*
  - Yes (*If yes, can you specify?*)
  - Maybe

- I do not know

Other interests beyond cyber security

- *Are there any other educational and professional paths that you would consider as an alternative to cyber security?*
  - No, if I can and want to, I would stay in cyber security
  - Yes, I am interested in cyber security, but there are other topics and careers that interest me at the same level
  - Yes, I am interested in cyber security, but there are other topics and careers that interest me even more

What other topics and careers are you interested in? Select at least one

- Artificial intelligence
- Programming (generic)
- Internet of Things
- Operations research
- Formal languages and compilers
- Databases
- Software engineering
- Computing infrastructures
- Algebra and mathematicsematical logic
- ICT for control systems engineering
- Distributed systems
- Digital project management
- Other

Educational and career paths beyond the CCIT

- *Compared to February 2020, have you changed your student or occupational status?*
  - No, I am still enrolled at the same high school or university degree
  - Yes, I graduated from high school and I am now enrolled at university
    - *Did you enroll in a computer science degree?*
      - Yes, and I want to enroll in cyber security courses*
      - Yes, but I do not want to enroll in cyber security courses*
      - I would have liked it, but I did not find any
      - I would have liked, but I did not have the financial means to do it
      - No*
      - Other

**Did the CCIT had a role in this choice? How?*

  - Yes, I graduated from my bachelor's degree and I am now enrolled in a master's degree
    - *Did you enroll in a cyber security master's degree?*
      - Yes*
      - No, but I want to enroll in cyber security courses*
      - I would have liked it, but I did not find any
      - I would have liked it, but it is too hard to get admitted
      - I would have liked it, but I did not have the financial means to do it
      - No*

**Did the CCIT had a role in this choice? How?*

  - Yes, I am looking for a job or I have started working

- *Have you started working in cyber security or other close fields?*
  - Yes*
  - No, but I want to progressively specialize in cyber security*
  - I would have liked it, but I could not find any opportunity in this sector
  - No*

**Did the CCIT had a role in this choice? How?*

Effect of CCIT on cyber security interest

- *How did the CCIT influence your interest in cyber security as a topic?*
  - The CCIT has significantly increased my interest in cyber security as a topic
  - The CCIT has increased my interest in cyber security as a topic
  - The CCIT has neither increased nor decreased my interest in cyber security as a topic
  - The CCIT has decreased my interest in cyber security as a topic
  - The CCIT has significantly decreased my interest in cyber security as a topic

Briefly describe how the CCIT influence your interest in cyber security as a topic.

- *How did the CCIT influence your interest in cyber security as a career opportunity?*
  - The CCIT has significantly increased my interest in cyber security as a career opportunity
  - The CCIT has increased my interest in cyber security as a career opportunity
  - The CCIT has neither increased nor decreased my interest in cyber security as a career opportunity

- The CCIT has decreased my interest in cyber security as a career opportunity
- The CCIT has significantly decreased my interest in cyber security as a career opportunity+

Briefly describe how the CCIT influence your interest in cyber security as a career opportunity.

Annex III: Reasons a regression discontinuity analysis would not work

The RDD works under the assumption that an objective allocation rule has been established and participants are divided into treatment and control group based on this rule. Participants usually perform a “test” before the intervention and, based on an assignment or cut-off score, they are assigned into the control or the treatment group. The scores have to be annotated as the analysis then is mainly concentrated on those who were “only just eligible” and the “not quite eligible” (Owen et al., 2011). The assumption here is that only people close enough to the assignment score are almost equivalent and therefore the main obstacle in using an RDD is that results only apply to those close to the cut-off.

In the CCIT, the admission test is an objective criterion, but an RDD might not be the most suitable design. Students pass the *in-situ* admission test (and receive the treatment/intervention) only if they are in the top 20 of students performing the local university test. Hence, we can have a situation in which a student that scores 90 points at the University of Bologna is ranked 21st in the local table (and therefore he is excluded from the program) whereas a student at the University of Milan scores 90 and ranks 15th in the local table (and therefore she is included in the program). In other words, it is not a cut-off score at the national level that determines whether they are accepted in the program, but their position in the ranking at the local university. To make an RDD work, one would need to know how students did their test and compare the near misses with those that will be accepted, but still, any results will likely be confounded by the “quality” of the university. Thus, the “quality” of the university is a variable determining who receives the intervention and who does not.

Moreover, on a more practical level, an RDD would work only if students were aware and or could recall their test scores. After the admission test, students are told whether they have passed the test or not, but they are not communicated their scores. As I will be directly administering the survey (and not the CCIT organizers)

to students, it would be impossible to link their admission test scores to the survey data they will provide as students will not be aware of their admission test results.

This makes a comparison based on test scores impossible.

Annex IV: Interview scripts

"Before" questionnaire (March 2020):

Background information:

1. What type of high school are/were you enrolled in?
   - Why did you make this choice?
   - What subjects do/did you prefer and why? Which ones instead you do/did not like?
   - Have you ever studied computer science in high school? What have you learnt?

2. (For university students only) What type of degree are you currently enrolled in?
   - Why did you make this choice?
   - What subjects do/did you prefer and why? Which ones instead you do/did not like?
   - Have you ever studied computer science at university?

3. At what age and how have you started using a computer?
   - What were, and what are, the main activities in which you use a computer? Are any of these activities somehow linked to cyber security?

4. Has at least one of your parents studied and/or worked in a technology-related occupation?

- If yes, how has this shaped your interest for computer science and/or cyber security?

5. Have you ever been enrolled in a cyber security course?
   - Why?
   - What have you learnt?
   - After this course, have you ever thought of deepening your cyber security interest? How?

6. Have you ever attended a computer science and/or cyber security competition?
   - What were the main reasons?
   - How did you find it?
   - What were the main positive and negative aspects?

7. Have you ever worked in a computer science and/or cyber security related job (even for a short term)?
   - In what tasks were you involved?

Cyber security interest and professional opportunities:

8. Are you interested in cyber security?
   - If yes, can you provide concrete examples of your interest?
   - Can you describe the process whereby you have become interested in cyber security by highlighting the most important moments?

9. Would you say you have already developed cyber security knowledge and skills?
   - How have you learned about cyber security topics and skills?

10. If you could quantify your interest in cyber security as a topic, what score would it get from 1 to 10?

11. Would you be interested to continue learning and obtain a degree in cyber security?
    - If yes, what kind of degree are you interested in? Why?
    - Have you ever thought about alternative degrees to cyber security? Which ones? Why?

12. Would your parents be supportive if you decided to get a degree in cyber security?

13. Have you ever thought of potentially becoming a cyber security professional one day? Can you please specify the following
    - What type of role?
    - What type of sector?
    - What type of organization?

14. If you could quantify your interest in cyber security as a career opportunity, how would it rank from 1 to 10?

15. Do you see any particular obstacle that may impede you to obtain a cyber security job, if you so you wanted?

16. Would your parents be supportive if you wanted to become a cyber security professional?

17. Are there any alternative professional careers in alternative to cyber security that you have ever thought of?

The CyberChallenge.IT experience

18. For what reason did you apply to the CCIT?
    - How did you come to know about this opportunity?

19. Do you believe that the CCIT will influence/might have influenced (for the control group) your interest in cyber security as a topic? How?

20. Do you think that the CCIT will make/could have made (for the control group) you understand better what kind of job opportunities the cyber security sector might offer? How?

"After" questionnaire (October 2020):

Questionnaire for the control group

The CCIT experience

1. What do you think of the admission process?
    - What did you like and what did you not like?
    - Is the admission process valuable to recruit people who can potentially have a career in the cyber security sector?

2. How was your reaction after knowing you had not been admitted?

3. Have you enrolled in the OpenCyberChallenge.IT programme or have you done any activity related to cyber security/computer science in this period?

4. In this period, have you developed cyber security knowledge and skills? If yes, would you say you need to further improve them? How?

Cyber security interest

5. Complete this sentence: If in February I gave to my cyber security interest a score of …, now I give it a score of … .

6. Did your CCIT experience change your interest in cyber security as a topic/study subject? How? Would you say your cyber security interest would have changed if you had been admitted to the CCIT training?

7. Would you be interested to continue studying and obtaining a cyber security degree? If yes, can you specify:
    - What type of course
    - Which university
    - What is the reasoning behind it

8. Do you see any obstacle that might impede you to obtain a cyber security degree?

9. Are there any educational paths in alternative to cyber security that you have considered?

10. Complete this sentence: If in February I gave to my cyber security career interest a score of …, now I give it a score of …

11. Did your CCIT experience change your interest in a cyber security career? How? Would you say your cyber security career interest would have changed if you had been admitted to the CCIT training?

12. Are you interested to become a cyber security professional? Can you specify:
    - What type of role
    - What type of sector
    - What type of organization

13. Do you see any particular obstacle that might impede you to obtain a cyber security job one day?

14. Are there any alternative professional opportunities/jobs you have considered?

15. Compared to February 2020 when you did the CCIT admission test, have you changed your student status? For example:
    - Did you enrol in a computer science degree?
    - Did you enrol in a cyber security master's degree?
    - Did you start working in cyber security or any other close sector?
    - Did the CCIT influence your choice?

16. What your next academic and professional steps? Is there anything in the cyber security field?

Questionnaire for the treatment group

The CCIT experience

1. What do you think of the admission process?
    - What did you like and what did you not like?
    - According to the CCIT training and the competitions you attended, is the admission process valuable to recruit people who can work in the cyber security sector?

2. Describe how was the training at the local university. For example:
    - Have you learnt new cyber security knowledge and skills? Do you think you still need to develop them? How?
    - How was your relationship with the instructors?
    - How was your relationship with your colleagues?
    - Overall what were the positive and negative aspects?

- How do you think your CCIT experience would have been without Covid-19?

3. Did you attend the local challenge?
    - How was your experience?
    - What were the main elements?
    - What were the main positive/negative aspects?
    - Do you think the training prepared you well to the local challenge?

4. Did you attend the national challenge?
    - How was your experience?
    - What were the main elements?
    - What were the main positive/negative aspects?
    - Do you think the training prepared you well to the national challenge?

5. Were there other activities/projects apart from the CCIT which you were a part of during the CCIT training?

Cyber security interest and careers

6. Complete this sentence: If in February I gave to my cyber security interest a score of …, now I give it a score of … .

7. Did your CCIT experience change your interest in cyber security as a topic/study subject? How?

8. Would you be interested to continue studying and obtaining a cyber security degree? If yes, can you specify:
    - What type of course
    - Which university
    - What is the reasoning behind it

9. Do you see any obstacle that might impede you to obtain a cyber security degree?

10. Are there any educational paths besides cyber security that you have considered?

11. Complete this sentence: If in February I gave to my cyber security career interest a score of …, now I give it a score of …

12. Did your CCIT experience change your interest in a cyber security career? How?

13. Are you interested to become a cyber security professional? Can you specify:
    - What type of role
    - What type of sector
    - What type of organization

14. Were there any CCIT scheduled activities aimed at presenting cyber security careers?

15. Did you upload your CV to the CCIT portal? Have you been contacted by any employer?

16. Do you see any particular obstacle that might impede you to obtain a cyber security job one day?

17. Are there any alternative professional opportunities/jobs you have considered?

18. Compared to February 2020 when you did the CCIT admission test, have you changed your student status? For example:
    - Did you enrol in a computer science degree?

- Did you enrol in a cyber security master's degree?
- Did you start working in cyber security or any other close sector?
- Did the CCIT influence your choice?

19. What your next academic and professional steps? Is there anything in the cyber security field?

Annex V: CUREC application form

The University of Oxford places a high value on the knowledge, expertise, and integrity of its members and their ability to conduct research to high standards of scholarship and ethics. The research ethics clearance procedures have been established to ensure the University is meeting its obligations as a responsible institution. They start from the presumption that all members of the University take their responsibilities and obligations seriously and will ensure that their research involving human participants is conducted according to the established principles and good practice in their fields and in accordance, where appropriate, with legal requirements. Since the requirements of research ethics review will vary from field to field and from project to project, the University accepts that different guidelines and procedures will be appropriate.

- Please check **"Where and how to apply for ethical review"** and the **CUREC flowchart** first to see if you need ethics approval.
- Please complete this form using a word processor and email it, together with your supporting documents, to your **Departmental Research Ethics Committee (DREC)** (**if applicable**). If you don't have a DREC please email this form to **ethics@socsci.ox.ac.uk** using your official **ox.ac.uk email** address. **Only type-written, emailed applications will be accepted.**

SECTION A: Filter for CUREC 2 application This section determines whether your study raises more complex issues requiring the completion of a full application for ethical review, known as the CUREC 2 application. **(Please mark 'X' in the Yes/No column.)**		
1. Are research participants classed as **people whose ability to give free and informed consent is in question**? (This may include under 18s (although see "competent youths"), prisoners, or adults "at risk".) Your attention is drawn to the University's **Safeguarding Code of Practice** and its implications for researchers involving children or adults at risk. This includes the need for the work to be risk assessed and for researchers to undertake related training. (**Note**: If any of your participants are aged 16 or under, answer 'Yes' here **and** also answer question 5 below.)	Yes ☐	No ☒
2. By taking part in the research, will participants be at risk of criminal prosecution (e.g. by providing information on drug abuse or child abuse)?	Yes ☐	No ☒
3. Does the research involve the **deception** of participants?	Yes ☐	No ☒

4. Does your research raise issues relevant to the **Counter-Terrorism and Security Act (the Prevent duty)**, which seeks to prevent people from being drawn into terrorism? Please see advice on this on our **Best Practice Guidance web page**.	Yes ☐	No ☒
If you answered 'No' to all the questions above, go to **Section B**. If you answered 'Yes' to any question above, continue to question 5 below.		
5. Is your project covered by a CUREC **Approved Procedure** (formerly known as "CUREC Protocols")?	Yes ☐	No ☐
If yes, give the specific Approved Procedure number(s):		
If you answered '**Yes'** to **ANY** of questions **1-4**, **and** answered '**No'** to question **5**, **stop completing this checklist and do not submit it for ethical review**. Instead, complete the CUREC 2 application form from the CUREC website, then submit that for ethical review. If you answered '**Yes'** to ANY of questions 1-3, **and** answered '**Yes'** to question 5, go on to **Section B**.		

SECTION B: Contact details and project description	
Contact details:	
1. **Principal investigator** OR supervisor (if student research) (give title and full name)	Gearon, Liam Keep, Ewart Martin, Andrew
2. Name of student (if student research)	De Zan, Tommaso
3. Degree programme (if student research), e.g. BA, BSc, MSc, MPhil, DPhil	DPhil
4. Department or Institute name	Education
5. Address for correspondence (if different from above)	Linacre College, St Cross Road, OX1 3JA, Oxford, United Kingdom
6. University (**not** private) e-mail address and telephone number	tommaso.dezan@linacre.ox.ac.uk
7. Name and status of others taking part in the project (e.g. third year undergraduate; postdoctoral research assistant)	-

Project description:	
8. Title of research project	Do cyber security competitions affect students' interest in a cyber security career? The cyber security skills shortage and public policy interventions
9. List of location(s) where project will be conducted	Oxford, United Kingdom
10. If your research involves overseas fieldwork or travel and your department requires a travel risk assessment, will you have completed and returned a risk assessment form beforehand? (This must be approved by your department before you travel. If you are travelling overseas, you are strongly advised to take out University travel insurance.) Please also address any	Yes ☐ No ☐ Not required in this instance ☒

physical or psychological risks for Oxford researchers and local fieldworkers in Section 16 below and discuss with your safety officer.	
11. Anticipated duration of overall research project	23 months
12.a) Anticipated start and end dates of the part of the research project involving human participants and/or personal data	From: 01/02/2020 To: 31/12/2021 **Note**: You will need ethics approval **before** you start your research. CUREC 1As may take up to 30 days to process. **Retrospective ethics approval cannot be granted.**
12. b) In the case of international or collaborative research, will you submit or have you submitted this project for ethical review or consideration elsewhere (e.g. collaborator's/local ethics committee, or other local approval)?	Yes ☐ No ☐ If 'Yes', please attach ethics or other approvals and give more details below. If 'No', please explain your reasons below. Please also refer to the Best Practice Guidance on Ethical Review of social-sciences based research conducted outside the UK (BPG 16), which includes an Ethics Issues Checklist for International Research (Appendix A)
13. **External** organisation funding the research (if applicable)	

14. a) Title and brief description of **research** (about 150 words) in lay language.
When describing the research, include your methodology, how you are applying professional guidelines, and the use to which results/data will be put. **Please also declare any conflicts of interest here.**

Title: "Do cyber security competitions affect students' interest in a cyber security career? The cyber security skills shortage and public policy interventions"

Context and methodology: There is a lack of cyber security professionals in the labour market, the so-called cyber security skills shortage and governments have established cyber security competitions to encourage young people to pursue a career and nurture their interest in cyber security. But do cyber security competitions do so? Evidence is mixed. This dissertation seeks to answer the following questions: do competitions affect students' interest in a cyber security career? How and why they do so? Ultimately, are they a viable solution

to thwart the shortfall of professionals? This dissertation answers these questions through a before and after, mixed-methods quasi-experiment, with data collected from the Italian national cyber security challenge.

Professional guidelines: This research adheres to the British Educational Research Association Ethical Guidelines for Educational Research and follows Oxford University's best practice guidances, especially BPG 04 Competent youths, BPG 06 Internet-based research and BPG 09 Data collection, protection and management.

Use of research data: The final dissertation will be deposited in the Oxford University Research Archive (ORA) as per University regulation. Results may be published in academic outlets such as the *Journal of Cybersecurity* or the *Journal of Cyber Policy*.

14.b) Description of participants and how you will **obtain informed consent** to take part in the research (about 200 words in total)

1. Description of participants **and** your criteria for inclusion/exclusion

Participants are students aged between 16 and 23 years-old participating to the Italian national cyber security competition, namely CyberChallenge.IT (CCIT). The research is divided in quantitative and qualitative parts.

For the quantitative part, all the students signing up online to the CCIT will be invited to complete an online survey before and after the competition takes place (in February and July 2020).

For the qualitative part, I aim to interview approximately 30 students based on whether they have accessed the competition or not. I will interview 15 students that have access to the competition and 15 students that, despite signing up online, are unsuccessful in accessing the competition.

2. Your method(s) of recruitment

For the quantitative part, all the students signing up online to the CCIT will be invited to complete two online surveys (before and after the competition). A weblink to the survey will be sent to participants by CCIT's organizers through the competition's web portal.

For the qualitative part, students will be recruited through the survey. The final question of the first survey will ask people that are interested in the research project to send an email and get in touch. I will encourage participation through the award of an Amazon voucher. Interviews will be done before and after the competition and will be conducted and recorded via Skype. Interviews will be later transcribed.

3. Your processes for obtaining consent from participants

For the quantitative part, informed consent will be obtained before the online survey starts. There will be a participant information section where written information is combined with a short online consent process achieved by a few simple tick box questions to establish age and consent itself, in accordance with BPG 06 Internet-based research.

For the qualitative part, written informed consent will be obtained prior to the interview. I will send the participant information sheet and the written consent form via email and will ask the participant to sign it and return it to me before the interview takes place.

Please **attach separate supporting documents (in Word)** if appropriate for your research (English language versions only). Tick those you are submitting below. If appropriate supporting documents are not submitted, you will be asked to provide these separately, which may delay the ethical review process.

- ☒ Recruitment and advertisement material (e.g. a poster, social media recruitment text, or brief invitation letter/ email)
- ☒ Information for participants to read (or hear) before they agree to take part (e.g. written information or, if applicable, an outline oral information script).
- ☒ A document to record informed consent. Templates for written consent forms and/or oral information scripts (in case of an oral consent process) are available from the CUREC website
- ☒ Questions to be asked of participants (e.g. interview questions, or a preliminary scope of questions, or a sample questionnaire)
- ☐ (If relevant) debriefing document after participants have taken part
- ☐ If you feel the above approaches are not appropriate for your study, provide details on how you will obtain consent from participants
- ☐ Please complete section 15 if you cannot obtain informed consent

15. If you cannot obtain informed consent from participants according to CUREC guidelines and good practice in your discipline, please give a brief explanation and justification of this decision below.

16. What are the ethical issues connected with your research and what steps have you taken to address them? **Please do not answer 'none'.** We need to see evidence that you have identified potential ethical issues with respect to your research and have taken steps to address them. If applicable, please address:

- Participant burdens and/or risks

The main issue could be the collection of data from "children" aged between 16 and 17. However, the purpose of this study qualifies them as "competent youth." The University's best practice guidance "BPG 4 Competent Youth" says that examples of research where the class of competent youths generally apply is for research on attitudes to science and mathematics. The purpose of my dissertation is to identify whether cyber security competitions affect students' interest in a cyber security career. In the science education field, career interest is a topic that usually relates to the broader literature on attitude towards STEM disciplines and careers. Therefore, students between 16 and 17 years-old that will participate to this research should be "considered to have sufficient understanding of the project and its implications for them that they can make up their own minds about taking part, and have that opinion honored."

The information provided have been evaluated also against Approved Procedures A15 ("Teachers and teaching in educational setting") and A25 ("Non-invasive research methods with children).

Through the online surveys and interviews, this research will collect some indirect identifiers/background information. However, these data will not be associated with personal data such as names and/or personal emails at any point. Online survey data will be preceded by participant information/consent form, but the participant will not be asked to identify him/herself.

To the best extent possible, interviews should not include personal data. They will definitely not contain any sensitive data.

- Your own physical and psychological safety as a researcher or of fieldworkers you may employ (see the University's and Social Science Division's Safety in Fieldwork guidance)

Given the topic and data collection methods of this research, I have no concerns regarding my own physical or psychological safety.

- Data protection/ confidentiality (also see Section 18).

All personal and research data will be stored on an encrypted USB driver and backed up on the University's HFS service.

Research data will be anonymized and personal data such as name/surname will only be collected on consent forms in the forms of signatures.

To the best extent possible, interviews should not include personal data. They will definitely not contain any sensitive data.

Interviews will be transcribed using Trint (https://trint.com/), an automated transcription software. For information regarding Trint's data security policy, see section 18.

For further information see section 18.

For more guidance on ethical issues, please see
http://researchsupport.admin.ox.ac.uk/governance/ethics/resources

17. Will your research involve discussing sensitive issues? This could be information relating to race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activities.	Yes ☐	No ☒

If you answered 'Yes', make sure you include some supporting information (as directed in Section 14 b.) above, showing the range of questions covering these issues.

18. Management and handling of personal and other research data

For the purpose of completing this section, all information provided by participants is considered **research data**. Any research data from which participants can be identified is known as *personal data*; any personal data which is sensitive is considered *special category data*.

Management of **personal data** and **special category data** of human participants, either directly or via a third party, must comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, as set out in the University's Guidance on Data Protection and Research. In answering the questions below, please also consider the points raised in the Data Protection Checklist. For advice on research data management and security, please consult with the University's Research Data Team (researchdata@ox.ac.uk) and/or your local IT department, and the University's web pages on research data management.

a.) **Please mark 'X' against the data you will collect for your research**

Consent records (written consent forms, audio-recorded consent, assent forms (for research involving minors) including participant name	☒
Online consent (may be anonymous)	☒
Opt-out forms	☐
Contact details for research purposes only (destroyed when no longer needed for this research)	☒
Contact details kept for future studies	☐
Audio recordings (preferably using PIN-protected audio recorder and stored on device's hard drive)	☒
Video recordings	☐
Transcript of audio/video recordings	☒
Photographs	☐
Task results (e.g. paper/online tasks, diary completion)	☐

Questionnaire answers	☒
Field notes	☐
Other (please specify below)	☐

b.) For **each** of the types of data selected above, state how this will be physically transferred from where it is collected to a local secure storage site (and backed up as necessary). This includes paper records and data captured electronically.

Online consent: CCIT's participants will access surveys only after giving consent (i.e. thick-the-box online consent form prior to starting the survey), but it will be anonymous (i.e. the participant will not be asked to give name and/or email address).

Questionnaire answers: questionnaire answers will be collected and generated by Qualtrics, the survey tool in use by the Department of Education. Once survey data are generated, they will be stored on an encrypted USB driver and backed-up on the HFS service provided by the University.

Contact details for research purposes only: participant will be asked to email me in case they consent to be interviewed. Email addresses will be stored on the email provider's servers (likely Gmail) but not transferred anywhere else. Access to email will be protected by two-factor authentication.

Consent records (written consent forms, audio-recorded consent, assent forms (for research involving minors) including participant name: interviewees will send their written consent forms via email. Once received, the forms will be stored on an encrypted USB driver and backed-up on the HFS service provided by the University.

Audio recordings (preferably using PIN-protected audio recorder and stored on device's hard drive): interviews will be recorded using Skype's recording function. The audio file will then be stored on an encrypted USB driver and backed-up on the HFS service provided by the University.

Transcript of audio/video recordings: interview recordings will be transcribed using Trint (https://trint.com/), an online automated transcription software. Given the present research questions, interviews will definitely not include sensitive data and should not include personal details. After audio recordings will be uploaded on Trint's platform and the software will transcribe it using artificial intelligence. Once the transcription is completed, the user will be allowed to edit the transcription. After the editing, the file can be exported as a Word document. The Word file will then be stored on an encrypted USB driver and backed-up on the HFS service provided by the University.

Trint's data security management is fully certified to ISO 27001. They are also verified by SAM (US government vendor), Crown Commercial Service (CCS), Cyber Essentials and are PCI DSS compliant. Trint uses HTTPS (using TLS 1.2) for secure data upload, export and transfer. Data is encrypted at-rest using AES 256.
c.) How and where will **each type of data** be stored during the research (until the end of all participant involvement)? Describe the arrangements for ensuring confidentiality, i.e. location of storage (e.g. Nexus 365 OneDrive for Business, SharePoint), security arrangements and de-identification of such data. Do not store unencrypted data in freely available cloud services or unprotected USB drives.
All the aforementioned data will be stored on an encrypted USB driver and backed up on the HFS service provided by the University, with the exception of contact details (see below). Contact details for research purposes only: participant will get in touch via email in case they consent to be interviewed. Emails will be stored on the email provider's servers (Gmail) but not transferred anywhere else. Access to email is protected by two-factor authentication.
d.) Will you use a unique participant number on research data instead of a participant name? If **yes,** state whether or not you will retain a list of participant names against numbers (i.e. pseudonymisation via a linkage list). Where will the list be stored, and when will it be destroyed?
This is not necessary as there is no need to collect/know participant's names for the purpose of my research
e.) Who will have access to the research data?
Only me and potentially the PIs. PIs might have access to questionnaire answers and transcript of audio recordings, if so they request. Data will be stored by me and made accessible to PIs only through secure devices, namely where the data have been safely stored and processed (i.e. my encrypted USB drive and my laptop)
f.) If research data is to be shared with another organisation, how will it be transferred / disclosed securely?
Data will not be shared with other organisations.

g.) When and how will identifiable data (including audio/video recordings & photos) be destroyed or deleted? **Note:** Records of consent should be retained for a **minimum of three years after publication or public release**. Some funders may require longer periods (see http://www.dcc.ac.uk/resources/policy-and-legal/overview-funders-data-policies). If you wish to retain contact details in order to re-approach participants about future studies, you must detail this in information provided to them and obtain specific consent for this.		
Three years after the thesis is deposited in the ORA University archive		
h.) Please confirm that you will store **other research data** safely for at least 3 years after final publication or public release and adhere to any additional research funder policies. For more information about the University policies, please see the University's web pages on research data management. If '**Yes'**, please give details of who will store the data and on storage format, location and security. Note that open science is encouraged. If **'No',** please provide further details below.	Yes ☒	No ☐
Data will be stored on an encrypted USB driver.		
i.) Does your research involve the use of secondary (i.e. previously collected) data? Common sources of secondary data include censuses, information collected by government departments, organisational records and data that was originally collected for other research purposes (If "**No**", please go to section **19**.)	Yes ☐	No ☒
j.) Do you have data access agreements for the use of this secondary data? (If so, please attach these.)	Yes ☐	No ☐
k.) Is your use of this secondary data compatible with what data subjects/participants agreed that their data should be used for?	Yes ☐	No ☐

l.) Could this data be linked back to an individual or individuals? If yes, address how securely any personally identifiable data will be transferred to you, and where and for how long it will be stored during or after the research. Who will have access to it?	Yes ☐	No ☐
19. Publication and dissemination of research data		
How will you disseminate and feedback project outcomes at the end of the research?	Research outcomes may be published in academic journals such as the *Journal of Cyber Policy* and *Journal of Cybersecurity*. They might also be published on online blogs/newspapers such as The Conversation or cyber security related media outlets such as ComputerWeekly.	

SECTION C: Methods and procedures to be used	
Method used: Please ensure you have addressed any potential ethical issues related to these methods in Section 14 and in your Participant Information Sheet	**Please mark 'X'**
1. Analysis of existing records	☐
2. Snowball sampling (recruiting through contacts of existing participants)	☐
3. Use of casual or local workers e.g. interpreters	☐
4. Participant observation	☐
5. Covert observation	☐
6. Observation of specific organisational practices	☐
7. Participant completes questionnaire in hard copy	☐
8. Participant completes online questionnaire or other online task	☒
9. Using social media	☐
10. Participant performs paper and pencil task	☐
11. Participant performs verbal or aural task (e.g. for linguistic study)	☐
12. Focus group	☐
13. Interview	☒
14. Audio recording of participant (you will generally need specific consent from participants for this)	☒
15. Video recording of participant (you will generally need specific consent from participants for this)	☐
16. Photography of participant (you will generally need specific consent from participants for this)	☐

17. Others (please specify below)	☐

SECTION D: Professional guidelines and training		
1. In this section, please mark 'X' against at least one of the following professional guidelines you aim to adhere to. You should use the principles listed in your chosen guideline(s) in conducting your own research. **Note**: this is not an exhaustive list.		**Please mark 'X'**
Research specialism/ methodology	**Association and guidance document**	
Anthropology	Association of Social Anthropologists of the UK and Commonwealth	☐
Computer Sciences	ACM Code of Ethics and Professional Conduct	☐
Criminology	http://www.britsoccrim.org/ethics/	☐
Education	British Educational Research Association Ethical Guidelines for Educational Research	☒
Geography	Association of American Geographers Statement on Professional Ethics	☐
History	Oral History Society of the UK Ethical Guidelines	☐
Internet-based Research	British Psychological Society: Conducting Research on the Internet Association of Internet Researchers Ethics Guide ACM Code of Ethics and Professional Conduct Also see our Best Practice Guidance on internet-based research	☐
Law (Socio-Legal)	Socio-Legal Studies Association: Statement of Principles of Ethical Research	☐
Management	Academy of Management's Professional Code of Ethics	☐
Political Science	American Political Science Association (APSA) Guide to Professional Ethics in Political Science	☐

Politics	Political Studies Association. Guidelines for Good Professional Conduct	☐
Psychology	British Psychological Society Code of Ethics and Conduct	☐
Social Research	Social Research Association: Ethical Guidelines	☐
Sociology	The British Sociological Association: Statement of Ethical Practice	☐
Visual Research	ESRC National Centre for Research Methods Review Paper: Visual Ethics: Ethical Issues in Visual Research	☐
Other professional guidelines. Please specify the other guidelines used here*:*		☐

2. Please indicate what training in research ethics (or research methodology) the researchers involved with this study have received, e.g. the title of the course and date completed (online training available at http://researchsupport.admin.ox.ac.uk/support/training/ethics), or discussions between researchers and supervisors, if applicable.

Research Ethics at Oxford

Social Sciences and Humanities

Claudia Kozeny-Pelling, Research Ethics Manager

HT 2018

Course offered by the Centre for Doctoral Training in Cyber Security

SECTION E: Signatures or email endorsements (The SSH IDREC Secretariat accepts either option below. If you have a DREC, check which signature option it prefers.)

- **Option 1:** Email confirmations from a University of Oxford email address can be accepted. Separate emails should come from each of the relevant signatories as outlined below, indicating acceptance of the relevant responsibilities. **Pasted images of signatures cannot be accepted.**
- **Option 2:** Handwritten (wet-ink) signatures. Please scan them and the rest of the checklist pages to create a single PDF document and email to us.

Please ensure this checklist is signed by:

For staff research:	**For student research**:
1. **Principal investigator**	1. **Principal investigator (project supervisor)**
2. **Head of Department (or nominee)**	2. **Head of Department (or nominee)**
	3. **Student researcher**

1. **Principal Investigator signature/supervisor signature (if student research)**

I understand my responsibilities as **principal investigator** as outlined in the CUREC glossary and guidance on the CUREC website.

I declare that the answers above accurately describe the research as presently designed, and that a new checklist will be submitted should the research design change in a way which would alter any of the above responses so as to require completion of CUREC 2 (involving full scrutiny by an IDREC). I will inform the relevant IDREC if I cease to be the principal investigator on this project and supply the name and contact details of my successor if appropriate.

Signature (or email endorsement using the above declaration):

……..

Print name (block capitals): Liam Gearon **Date**: 12/11/2019

2. **Departmental endorsement signature**

I have read the research project application named above. On the basis of the information available to me, I:

(i) consider the principal investigator to be aware of her/his ethical responsibilities in regard to this research;

(ii) consider that any ethical issues raised have been satisfactorily resolved or are covered by relevant professional guidelines and/or CUREC approved procedures, and that it is appropriate for the research to proceed (noting the principal investigator's obligation to report should the design of the research change in a way which would alter any of the above responses so as to require completion of a CUREC 2 full application);

(iii) am satisfied that: the proposed project design and scientific methodology is sound; the project has been/will be subject to appropriate **peer review**; and is likely to contribute to existing knowledge and/or to the education and training of the researcher(s) and that it is in the **public interest**.

Signed by Head of Department or nominee *(example nominees for student research include the Director of Graduate Studies/ Director of Undergraduate Studies)*:

Signature (or email endorsement using the above declaration):
……

Print name (block capitals): **Date**: 12/11/2019

3. **Student signature (if student research)**

I understand the questions and answers that have been entered above describing the research, and I will ensure that my practice in this research complies with these answers, subject to any modifications made by the principal investigator properly authorised by the CUREC system.

Signature by student (or email endorsement using the above declaration):
……..

Print name (block capitals): Tommaso De Zan **Date**: 12/11/2019

Annex VI: Consent forms

Survey research information/privacy note and consent form

"The cyber security skills shortage and public policy interventions: The impact of cyber security competitions on interest"

PARTICIPANT INFORMATION SHEET

Department of Education Research Ethics Committee (CUREC) Approval
Reference: ED-CIA-20-047

1. ***Why is this research being conducted?***

   There is a lack of cyber security professionals in the labour market, the so-called cyber security skills shortage, which puts countries' economic development and national security at stake. Among the public policies most used by governments to tackle it, cyber security competitions have been established to encourage young people to pursue a career and nurture their interest in cyber security. But do they? This dissertation seeks to answer the following questions: do competitions affect students' interest in a cyber security career? How and why they do so? Ultimately, are they a viable solution to thwart the shortfall of professionals?

2. ***Why have I been invited to take part?***

   You have been invited because you signed up to CyberChallenge.IT and you sent an email to ccitoxford@gmail.com confirming your willingness to be interviewed.

3. *Do I have to take part?*

No. You can ask questions about the research before deciding whether or not to take part. If you do agree to take part, you may withdraw yourself from the study at any time, without giving a reason, by advising me of this decision via email.

The deadline by which you can withdraw any information you have contributed to the research is **26th July 2020**. Until the point of withdrawal, the data obtained from you will be stored safely on an encrypted USB driver and backed up on the University of Oxford's HFS service. The data will be processed and analysed for the sole purpose of the research and results stemming from your data will not be published prior to **26th July 2020**.

In case you withdraw from this study, however, we are unable to offer you an Amazon voucher.

4. *What will happen to me if I take part in the research?*

If you are happy to take part in the research, you will be interviewed via Skype two times: in March and July 2020. Before the first Skype interview, I will send you the project's information sheet (the paper you are reading right now) and the consent form for you to review and sign.

If you are still happy to take part, I will ask you to sign the consent form and send it to me via email before the Skype interview takes place. *If you are below 18-years old, you must inform your parents about your participation and make them read this participant information sheet.*

Before starting our interview, I will talk you through the study procedures and give you the chance to ask any questions. The interview sessions should take approximately 45 minutes for each interview, in total 90 minutes for the 2 interviews. You can also ask to pause or stop the interview at any time.

With your consent, I would like to audio record you so that I can have an accurate record of your thoughts. I would like your permission to use direct quotes [and for your name to be attributed to these against a pseudonym] in any research outputs. I would like your permission to use **anonymised data** in future studies, and to share data with other researchers (e.g. in online databases). All personal information that could identify you will be removed or changed before information is shared with other researchers or results are made public.

5. ***Are there any potential risks in taking part?***

The collected data will be stored electronically, but they will be anonymised to avoid breach of confidentiality/data protection issues. They will be stored electronically in a secure database and backed up using the University of Oxford's HFS service.

6. ***Are there any benefits in taking part?***

You will receive a €20 Amazon voucher if you complete both interviews and a final survey in July. If you do not complete either one of the two interviews or the final survey, unfortunately you will not receive the Amazon voucher.

7. ***What happens to the data provided?***

The information you provide during the study, such as survey answers and recordings from interview, is the research data. Any research data from which you can be identified – such as the audio recording of your interviews or the email addresses you used to send a message to ccitoxford@gmail.com – is known as personal data.

Personal data will be stored on an encrypted USB device and backed up on the University of Oxford's HFS service. They will be stored for three years upon submission of this research in the form of DPhil dissertation in the Oxford Research Archive in fulfilment of Oxford University's regulations. Other research data

(including consent forms) will be stored for at least 3 years after publication in the Oxford Research Archive as per the University of Oxford's regulation.

The researcher and the principal investigator (i.e. supervisor) will have access to the research data. Responsible members of the University of Oxford may be given access to data for monitoring and/or audit of the research.

8. *Will the research be published?*

The research may be published in academic journals such as the *Journal of Cyber Policy* or the *Journal of Cybersecurity* or in online scientific blogs and newspapers.

The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, has established an online archive of research materials. This archive includes digital copies of student theses successfully submitted as part of a University of Oxford postgraduate degree programme. Holding the archive online gives easy access for researchers to the full text of freely available theses, thereby increasing the likely impact and use of that research.

The research will be written up as a student's DPhil thesis. On successful submission of the thesis, it will be deposited both in print and online in the University archives to facilitate its use in future research. If so, the thesis will be openly accessible.

9. *Who has reviewed this study?*

This study has been reviewed by, and received ethics clearance through, the Department of Education Research Ethics Committee (CUREC). Approval Reference: ED-CIA-20-047

10. ***Who do I contact if I have a concern about the study or I wish to complain?***

If you have a concern about any aspect of this study, please contact:

Tommaso De Zan

tommaso.dezan@linacre.ox.ac.uk

and we will do our best to answer your query. I will acknowledge your concern within 10 working days and give you an indication of how it will be dealt with.

If you remain unhappy or wish to make a formal complaint, please contact the Chair of the Research Ethics Committee at the University of Oxford's Department of Education who will seek to resolve the matter as soon as possible:

Chair of the Education Departmental Research Ethics Committee

research.office@education.ox.ac.uk.

Department of Education

University of Oxford

15 Norham Gardens

Oxford, OX2 6PY

Phone +44 (0) 1865 274024

Fax +44 (0) 1865 274027

11. ***Data Protection***

The University of Oxford is the data controller with respect to your personal data, and as such will determine how your personal data is used in the study.

The University will process your personal data for the purpose of the research outlined above. Research is a task that is performed in the public interest.

Further information about your rights with respect to your personal data is available from https://compliance.web.ox.ac.uk/individual-rights.

12. ***Further Information and Contact Details***

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

Tommaso De Zan
tommaso.dezan@linacre.ox.ac.uk
Department of Education
University of Oxford
15 Norham Gardens
Oxford, OX2 6PY
Phone +44 (0) 1865 274024
Fax +44 (0) 1865 274027

Tick the following boxes to confirm that:

1. I am at least 16 and I have signed up to the 2020 CCIT edition;
2. I understood the research objectives, that data are anonymous, how they will be stored and analysed;
3. I understood who to contact to get more information and how to lodge a complaint.

Interview consent form

“The cyber security skills shortage and public policy interventions: The impact of cyber security competitions on interest”

PARTICIPANT CONSENT FORM

Department of Education Research Ethics Committee (CUREC) Approval Reference: ED-CIA-20-047.

Research abstract:

There is a lack of cyber security professionals in the labor market, the so-called cyber security skills shortage, which puts countries' economic development and national security at stake. Among the public policies most used by governments to tackle it, cyber security competitions have been established to encourage young people to pursue a career and nurture their interest in cyber security. But do they? This dissertation seeks to answer the following questions: do competitions affect students' interest in a cyber security career? How and why they do so? Ultimately, are they a viable solution to thwart the shortfall of professionals?

		Please tick each box
1	I confirm that I have read and understand the information note provided via email. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	☐
2	I understand that my participation is voluntary and that I am free to withdraw at any time prior to 26th July 2020, without giving any reason, and without any adverse consequences or penalty.	☐
3	I understand that research data collected during the study may be looked at by authorised people outside the research team. I give permission for these individuals to access my data.	☐

4	I understand that this project has been reviewed by, and received ethics clearance through, the University of Oxford Department of Education's Research Ethics Committee.	☐
5	I understand who will have access to personal data provided, how the data will be stored and what will happen to the data at the end of the project.	☐
6	I understand how this research will be written up and published.	☐
7	I understand how to raise a concern or make a complaint.	☐
8	I consent to being audio recorded	☐
9	I understand how audio recordings will be used in research outputs	☐
10	I agree to the use of pseudonymised quotes in research outputs	☐
11	I agree to take part in the study	☐
12	I agree for research data collected in this study to be given to researchers, including those working outside of the EU, to be used in other research studies. I understand that any data that leave the research group will be fully **anonymised** so that I cannot be identified.	☐
13	I agree that my **anonymised** personal contact details can be retained in a secure database so that the researchers can contact me about future studies.	☐

_____ dd / mm / yyyy _____

_____

Name of Participant	Date	Signature
Name of person taking consent	Date	Signature