

# National cyber security competitions to mitigate the skills shortage: the Italian CyberChallenge.IT

Tommaso De Zan

Senior Consultant in Digital Policy – ICF

ENISA Cybersecurity Skills Conference – 21<sup>st</sup> September 2022

# Who Am I?

Currently: Senior Consultant in Digital Policy at ICF

Previously:

- PhD student at University of Oxford and ENISA CEI Expert (2017-2022)
- Associate Fellow at the EUISS (2017)
- Researcher at IAI (2014-2017)

Academic background:

- PhD in Cyber Security and Education (University of Oxford)
  - Visiting student: Hertie School
- Master's degree in International Relations (University of Bologna)
  - Visiting student: Josef Korbel School of International Studies and Université catholique de Louvain
- Bachelor's degree in Political Science and International Relations (University of Bologna)

# What I will talk about today

Results and implication of my PhD thesis: *“Mitigating the cyber security skills shortage: The influence of national skills competitions on cyber security interest”*.

I will argue that: national cyber security skills competitions (NCSSCs) are “effective” tools to mitigate the shortage but should be part of a broader set of measures. Cyber security skills are “strategic” and more should be invested in developing them.

Presentation will follow this structure: 1) background; 2) research questions; 3) methodology; 4) results; 5) conclusions; and 6) implications.

# Background: “the cyber security skills shortage”

Although evidence is not as strong as one might think, there are currently many issues affecting cyber security skills supply and demand in the labour market



The so-called “cyber security skills shortage” is affected by four main drivers **located in both the demand and supply sides:**

Education system’s inability to provide students with “the right” cyber security knowledge and skills;

Low number of students interested in cyber security as topic and as a career opportunity

Employers’ unrealistic expectations regarding pool of potential cyber security employees

Employers’ limited investments in cyber security human capital (i.e. training)

## Background: policies to tackle the shortage

- Hence, SOME governments, have implemented policy interventions to reduce the shortage of professionals: **national cyber security skills competitions (NCSSC) have sprouted.**
- However, the scientific literature has not provided a definitive assessment; it is unclear whether competitions are effective and what their effects are: *"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).

# 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?

# Methodology

I used the Italian CyberChallenge.IT (CCIT) as a case study. Why? One of the largest NCSSCs in Europe for number of people recruited and invited to training (in 2020 4454 and 560, respectively).

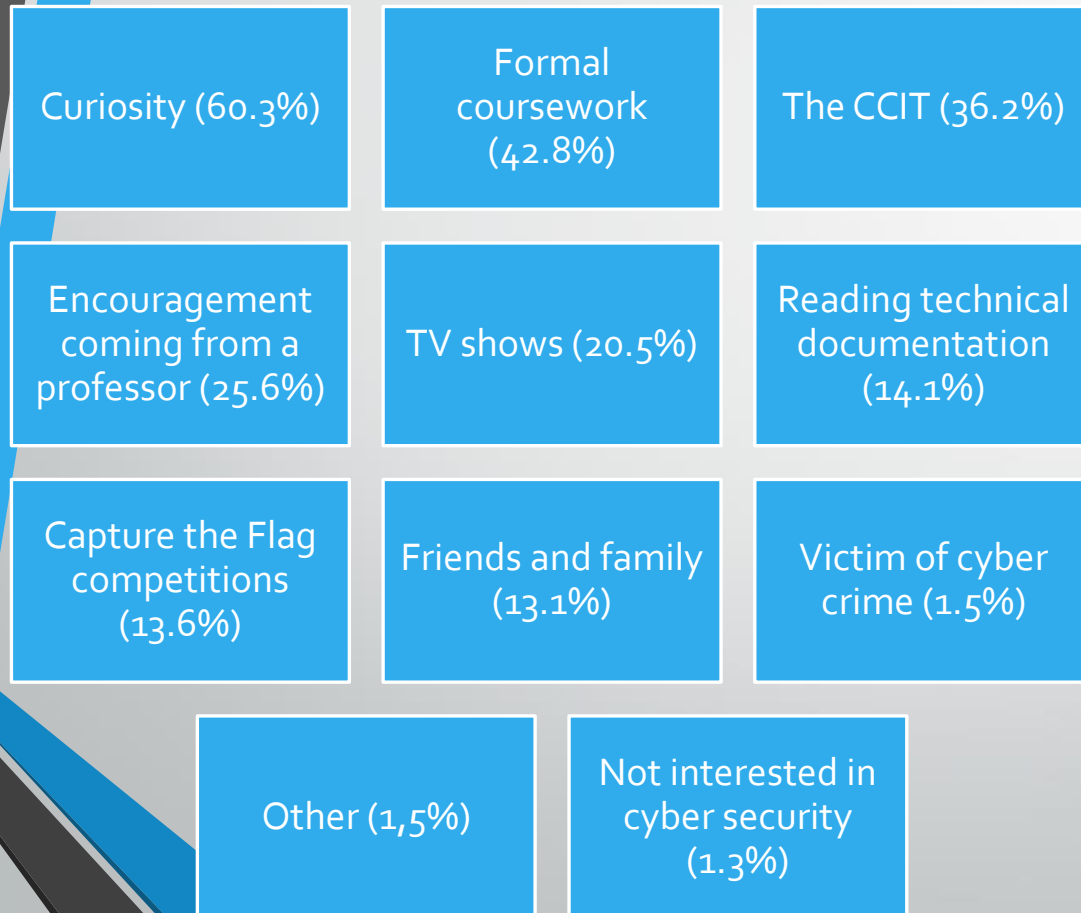
The research design followed the principles of an impact + process evaluations:

I collected data before and after the CyberChallenge.IT (2020 edition)

I collected survey (1285 replies) and interview data (50 interviews)

I collected data from non-randomized treatment (students who were selected and were trained) and control groups (students who were not selected)

# Results: How did participants develop an interest in cyber security before attending the CCIT?



About the role of the CCIT:

Approximately 1/3 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:

*"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."*



# Results: Did the CCIT influence participants' interest in cyber security as a topic and as a career?

- *“Did the CCIT influence your interest in cyber security as a topic?”*

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 (N=390);

- *“Did the CCIT influence your interest in a cyber security career?”*

62% of TG respondents stated that their cyber security career interest had either significantly increased or had increased by the CCIT, compared to 45% in the CG.

Please note: students reported that the CCIT increased interest in cyber security as a topic more than interest in cyber security as a career.

Results: What factors contributed the most to increase cyber security interest among CCIT participants?

Two main factors:

- 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**. The training went in-depth and was practical at the same time, touching upon topics that students would not have learnt by themselves.
- Interviewees also appreciated **the expertise and the helpfulness of instructors**.
- (Students had mixed reviews about the careers seminars).

# Results: What factors contributed the most to increase cyber security interest among CCIT participants? Some quotes

*"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."*



*"Even when they were not on duty, they were having fun with us (...) teaching even outside the normal class hours."*



*"More than instructors, they became friends, colleagues, because they were very helpful in answering questions they did not really know."*

## Other **key results**: little awareness and “competing interests”

- Students had **little awareness of the cyber security sector**, both in terms of educational offers and potential professional roles: Most respondents (45%) (N=390) did not know of any specific cyber security degree they could pursue (*“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”*)
- Students were interested in cyber security, but also other topics: only 16% (N=390) said they would consider to stay in the cyber security sector no matter what; 51% revealed that other topics and opportunities **interested them at the same level**, especially **artificial intelligence, programming and/or software engineering**.

# Conclusions

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.



However, it should:

Be part of a broader cyber security development system, which should foresee the inclusion of formal cyber security coursework in secondary and higher education curriculums and employers' cooperation;

Maintain 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

# Conclusions

Asking a NCSSC to solve the cyber skills shortage on its own would mean failing to understand the complexity of the problem and over-estimating what a single intervention can achieve.

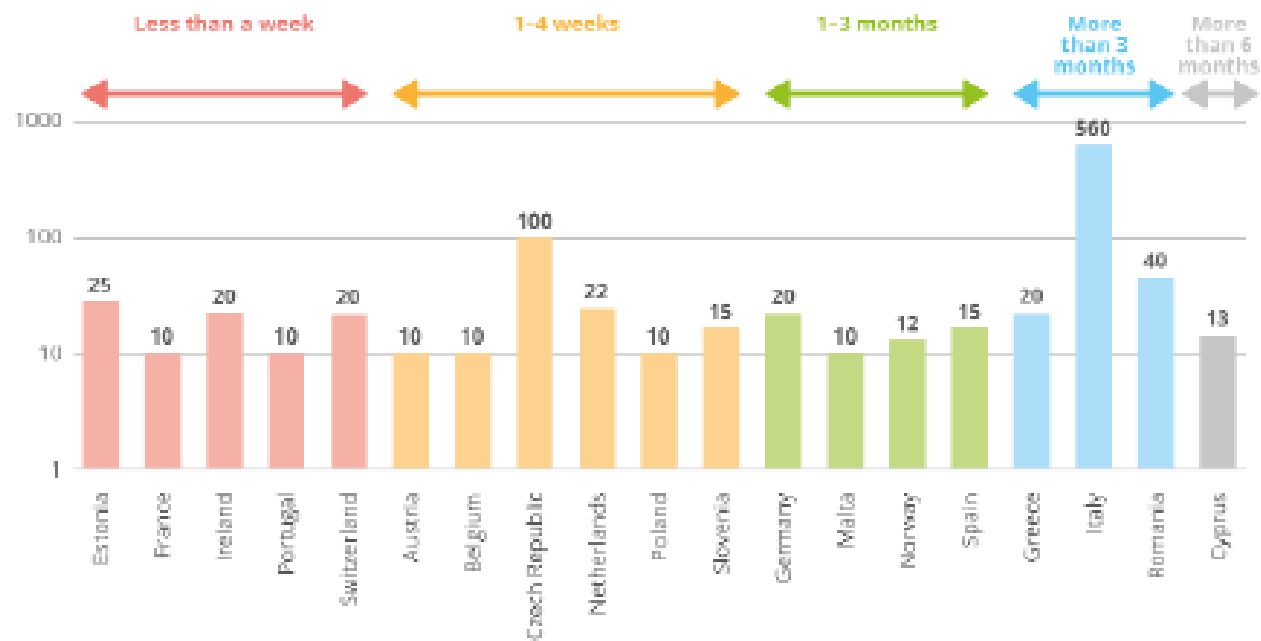
A NCSSC can neither be a substitute for a modern education system that is somehow reflective of labour market demands nor a panacea for employers with unrealistic expectations about the cyber security workforce.

A NCSSC should be one of the elements in a broader skills strategy that clearly understands the challenges posed by the skills shortage and has the resources and persistence to cope with it.

# Implications for the ECSC

NCSSCs are useful interventions to mitigate the shortage, should they be funded accordingly? An ENISA study (2021) found that **only 25%** of national organizers thought they **had enough financial resources** to achieve the competition's objectives.

Training was one of the main factors influencing interest in cyber security, so should all NCSSCs include cyber security training? Until 2021, most competitions were training too few students for too little time (ENISA, 2021)



Training provided by competitions with respect to time and number of participants trained (ENISA, 2021)



Why this is  
important?

Hard National Security Choices

LAWFARE

☰ TOPICS HOME FOB BLOG JAN. 6 PROJECT REVIEWS AND ESSAYS ▼ AEGIS RESOURCE PAGES ▼ MORE ▼

CYBERSECURITY

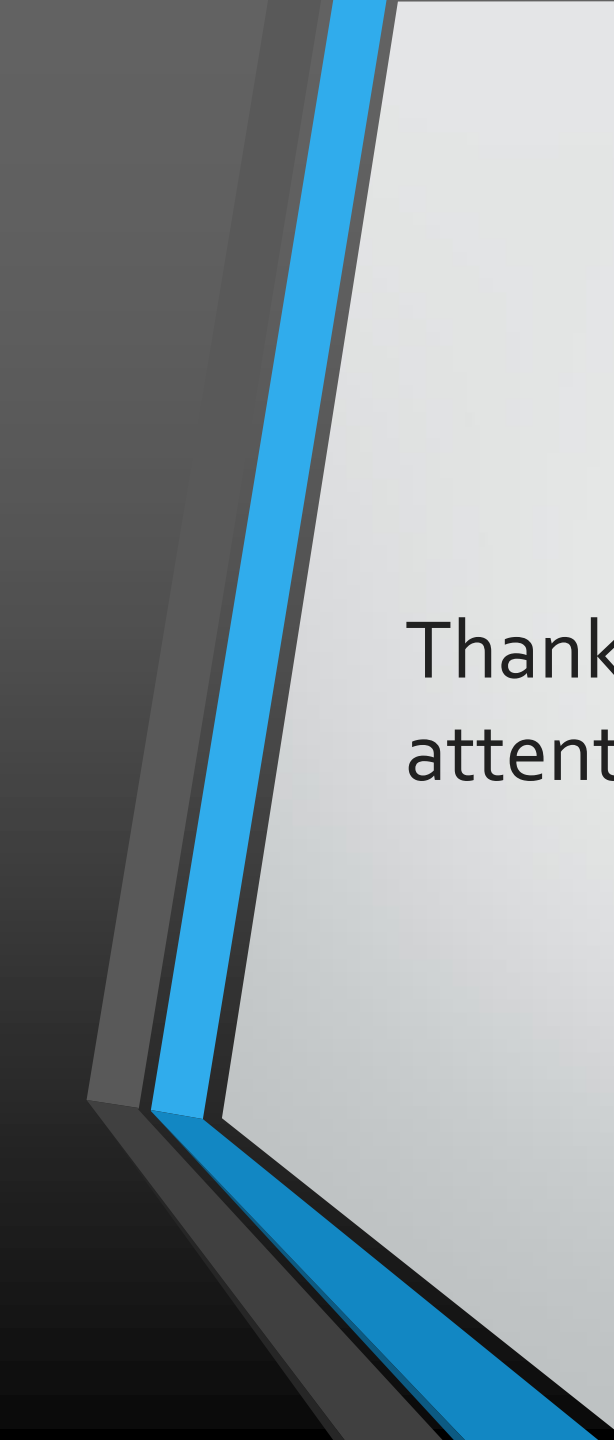
## The Strategic Relevance of Cybersecurity Skills

By **Tommaso De Zan** Monday, June 27, 2022, 8:01 AM

Cyber security  
skills are  
“strategic”  
and we should  
nurture them

*“America’s cybersecurity workforce is a strategic asset ... a superior cybersecurity workforce will promote American prosperity and preserve peace.” (White House, 2019).*

- If the cybersecurity workforce is a strategic asset that can promote prosperity and preserve peace, then **it follows that the lack of cybersecurity workers is a strategic issue with potential geopolitical implications.**
- In fact, if a country could significantly accrue its cybersecurity expertise by creating a proficient national cyber workforce, **it would gain a comparative advantage:** By nurturing the people with the right skills to fend off online attacks, that country **could continue enjoying the benefits of digital advancements,** as opposed to other countries that may struggle to defend themselves if they lack a security-savvy workforce.



Thanks for your  
attention!

- 15mins are short to summarise 4 years of research, so feel free to download my thesis "*Mitigating the cyber security skills shortage: The influence of national skills competitions on cyber security interest*" (Oxford University Research Archive, <https://bit.ly/3RWaXl2>)
- Other resources:
  - "The Strategic Relevance of Cybersecurity Skills" (2022, Lawfare, <https://bit.ly/3QOCCnL>)
  - "Future research on the cyber security skills shortage" (2020, Cyber Security Education Principles and Policies, <https://bit.ly/3r7PcDb>)
- Email me for any comment or feedback:  
[tommaso.dezan@icf.com](mailto:tommaso.dezan@icf.com)