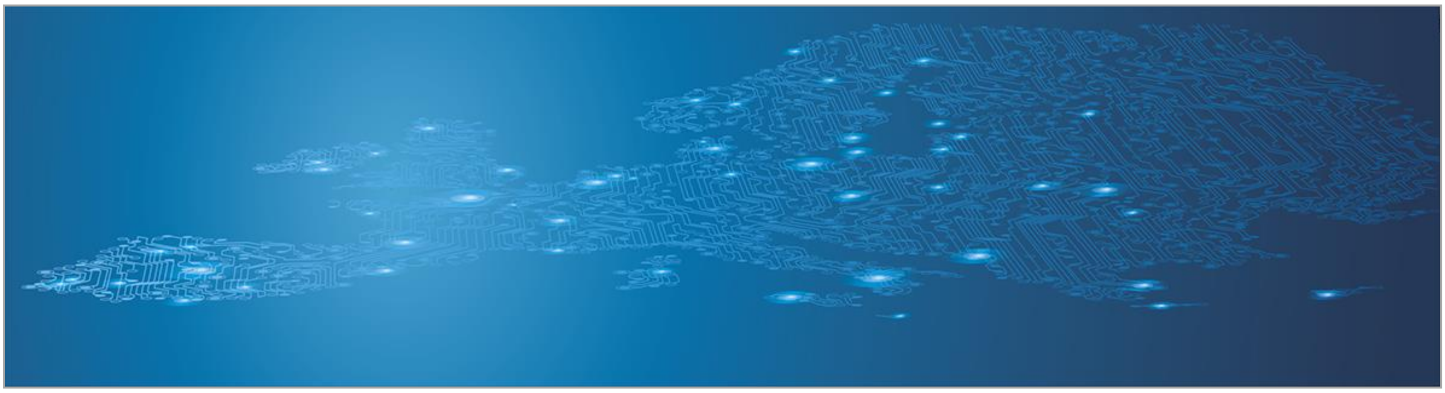
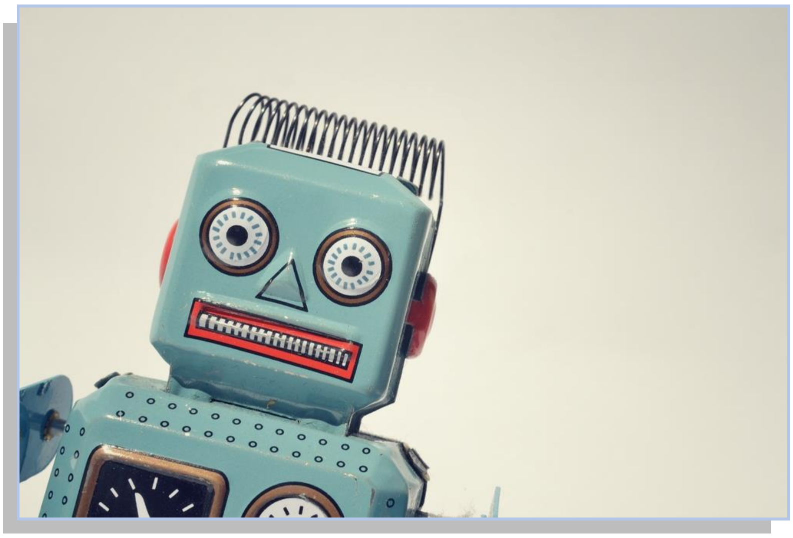




Cyber security competitions — the status in Europe

Recommendations for a pan-European approach

October 2014

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at http://www.enisa.europa.eu

Authors

Cyber Challenge Organising group (Joe Pichlmayr — Cyber Security Austria; Andrei Avădănei — DefCamp Romania; Ignacio Caño Luna and Raúl Riesco INTECO Spain; Okonweze Austen and Judy Baker — Cyber Security Challenge UK; Bernhard Tellenbach — Swiss Cyber Storm; Ilias Chantzos — Symantec; Daria Catalui and Demosthenes Ikonomou — ENISA)

Contact

To contact the editor: Daria Catalui stakeholderrelations@enisa.europa.eu

For media enquires about this paper: press@enisa.europa.eu

Acknowledgements

We would like to thank Professor Bettina Berendt of KU Leuven for her contribution to this report.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to Regulation (EU) No 526/2013. This publication does not necessarily represent the state of the art and ENISA may update it from time to time.

Third party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources, including external websites, referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained herein.

Copyright notice

Catalogue number TP-04-14-678-EN-N   ISBN 978-92-9204-091-8   doi:10.2824/32650

Executive summary

This report focuses on analysing the current situation concerning cybersecurity challenge competitions in Europe. The experience gathered will be the basis to develop a pan-European competition on cybersecurity.

The European Cyber Security Challenge Competition 2015 is set to be the result of a public–private partnership that comprises of capable players aiming at improving the ICT educational approach that digital citizens in Europe receive.

This report provides a general overview of existing cyberchallenge competitions in Member States. It also outlines a roadmap for a future pan-European cyberchallenge competition. The first part presents the experience of five countries. The second part comprises of a short ‘how to’ guide containing the steps in organising a challenge. The third part goes into more detail on concrete developments concerning a pan-European challenge. The fourth and final part contains several recommendations that should be taken into account. Graphics providing additional content can be found in annex.

The final recommendation underlines:

> *‘The importance of the European Commission’s active involvement in getting on board policymakers in Member States, the expertise of the EU’s cybersecurity agency, ENISA, in involving the best experts in the field and the responsibility of public and private stakeholders in understanding that the target is set very high and that they should engage to the best of their ability’.*

Contents

1. Introduction

This report focuses on the status of cyber challenge competitions in Europe and their implementation. The European Commission's joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Cybersecurity strategy of the European Union: an open, safe and secure cyberspace' ([1]) suggests that the Commission

> *organise, with the support of ENISA, a cybersecurity championship*

where university students will compete in proposing network and information security (NIS) solutions. In order to help develop the planning for this Europe-wide endeavour, this report provides information on current national efforts that can be used as the starting point for the pan European challenge.

Goal

The aim of this report is to provide up-to-date information about current cyberchallenge competitions taking place in Europe. The experiences of all the Member State will be considered later on, when establishing the general framework for the development of a pan-European competition for students.

Target audience

The primary audience for this report is national experts already involved in, or interested in, cyberchallenge competitions. However, the information within it will also be useful for a broader public including policymakers and NIS educators .

Structure

This report provides a general overview of existing cyberchallenge competitions in Member States, as well as a roadmap for a future pan-European cyberchallenge competition. The first part presents the experience of five countries. The second part comprises of a short 'how to' guide containing the steps in organising a challenge. The third part goes into more detail on concrete developments concerning a pan-European challenge. The fourth and final part contains several recommendations that should be taken into account. Graphics providing additional content can be found in the annex.

Additionally, the authors of this report are opening up a wider consultation and stakeholders interested in this work are invited to contact the Cyber Challenge Competition Committee in order to join the initiative ([2]).

[1] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (see in particular p. 8).

[2] Contact e-mail: stakeholderrelations@enisa.europa.eu

2. Presentation of existing cyberchallenge competitions in Europe

This chapter presents existing competitions and their results. Some basic information is contained in the table below.

Organiser	Name of the challenge	Date	Periodicity
Austria	Austrian Cyber Security Challenge	From May 2014 to November 2014	Annual
Switzerland	Swiss Cyber Storm	From May 2014 to November 2014	
Romania	D-CTF	From October 2014 to November 2014	
Spain	Spanish CyberCamp	From October 2014 to December 2014	
United Kingdom	Cyber Security Challenge	All year	

About Cyber Security Austria ([3])

'Cyber Security Austria — Association to promote the safety of Austrian strategic infrastructure' is a non-profit, independent and non-party organisation, whose goal is to sponsor and promote security awareness in Austria and to encourage the IT security of strategic infrastructure.The honorary members of the association want, in particular, to collect, link, facilitate and publish existing competencies.

About Swiss Cyber Storm ([4])

The message is ' Meet the future talent'.

Swiss Cyber Storm, founded on 15 November 2012, is a non-profit organisation that conducts the Swiss Cyber Storm IT security conferences and cybersecurity challenges. It organises the annual Cyber Security Challenge, whose 2014 edition will be the largest contest in the search for Switzerland's most promising young cybersecurity talents, to promote their abilities and to convince them to pursue a career in cybersecurity.

About Defcamp Romania ([5])

Defcamp Capture the Flag (D-CTF) is an innovative and ground-breaking security capture-the-flag (CTF) competition in central and eastern Europe. The most skilful hackers and IT geeks put their knowledge to the test and try to get into the 'best of the best' top five, in the hope that they can win the overall event or 'die trying'. There is one important rule — hack before getting hacked!

([3]) Further information at http://www.cybersecurity.at (currently only in German).

([4]) Further information at http://www.swisscyberstorm.com

([5]) Further information from Andrei Avădănei Andrei@defcamp.ro or at http://defcamp.ro and http://dctf.defcamp.ro

About Spanish Cyber Camp[6]

Spanish Cybercamp is a government sponsored event inside Cybersecurity Excellence Program of the spanish digital agenda and the confidence plan for promoting cyberskills talent of our future professionals in cybersecurity.

It is a cybersecurity challenge for best spanish students and researchers in cybersecurity as well as best international talented professionals by different competitions and advanced challenges designed by INTECO and several stakeholders. The event will allow the industry participation by presenting success cases.

The event (which first edition is scheduled from October to December 2014), include online challenges, training labs, CTF, wargames, hackathons as well as tracks to foster enterpreneurship in Cybersecurity with speed dating slots with investors.

In its first edition, the physical event will take place in December between 5th and 7th in Madrid.

About Cyber Security Challenge UK ([7])

Cyber Security Challenge UK Ltd is a not-for-profit company, formed in March 2010, to plug the cybersecurity skills gap in the United Kingdom. Some 90 % of professionals surveyed had difficulties in recruiting the cybersecurity talent needed by their companies, across all eight categories of cybersecurity jobs. Nearly 60 % predicted (correctly) an increase in the number of jobs in the UK cybersecurity market.

2.1 Workshop in April 2014

As a first step to kick off the work **([8])**, ENISA opened a public call and invited stakeholders to a common meeting. A workshop on 'Cybersecurity challenges in Europe' was organised on 29 April in Brussels. The main goal was to look at what is being done in the area of cybersecurity and how this could be coordinated. The talks, which lasted for half a day, covered a large range of initiatives throughout Europe for identifying (mostly young) people with a talent for advanced activities in cybersecurity — and for recruiting them to work in this area. Speakers gave an overview of activities including hackathons, red team/blue team and CTF games, SWOT analyses and speed dating. In addition to these more competitive styles, more standard university-level courses were described. Speed dating and forms of mentoring are two of the ways in which participants can enter into contact with professionals in the field, a factor that was recognised by many speakers as being extremely conducive to the success of the activities.

In Sections 2.2 to 2.7, the competitions presented at the workshop will be described in detail. The remainder of Section 2.1 contains additional observations and conclusions from the workshop.

All these activities focus on people who are suited to being security experts — but the actions (or non-actions) of non-expert computer or data users also determine security and privacy outcomes. This was the specific topic of a presentation at the workshop on the classification of security types, which outlined how too much attention is currently being paid to perimeter security — which means that once an attacker has gained access to the area inside the perimeter (premises, the computer system, etc.), there is a lot of potential damage, because management control, operational controls and internal security measures are often lacking. Interestingly, according to the presentation, this is very different in other security fields such as chemical, biological and nuclear security. It was pointed

([6]) Further information will be available at Website: http://cybercamp.es (publicly available from September 2014)

([7]) Further information at http://cybersecuritychallenge.org.uk/

([8]) Rapporteur Bettina Berendt, KU Leuven, Belgium (http://people.cs.kuleuven.be/~bettina.berendt).

out that training and awareness raising are needed, and that these activities have to take into account specific user needs and insights about human learning. Standards can play several roles in increasing security, including conveying the notion that an individual company or institution is not alone with specific security problems.

Other presentations also emphasised the need for 'specialised experts' of various kinds and mentioned the diversity of the target groups for concrete types of events. For example, Symantec's Cyber Readiness Challenge 'can accommodate very different levels of skills', and the DefCamp hacking conference recently started organising capture-the-flag exercises for children (DefCamp Kids). The Uk Cyber Security Challenge provides safe environments where people can test and demonstrate their skills; and showcases the spread of opportunities for future cyber defenders as well as informs participants about available education and training opportunities.

The short discussion centred on two, related questions. One was the question of how a hard-to-reach but important target group, a range of SMEs, could profit from the activities described. Cisco called on universities to use the Cisco courses also in teaching activities aimed at a wider audience (including SMEs), and Symantec offers awareness-raising tools for the general public. Another question was to what extent the didactic approaches described above could also be employed in training and awareness-raising for non-expert computer/data users. This might be beneficial because the didactic style is more hands-on and constructivist than the more frequently used 'lecture-style' teaching activities — and thus more likely to be successful in the area of security where not only knowledge but also practices shape outcomes. However, many questions will need to be addressed.

The restricted time of the workshop did not permit an in-depth discussion of this question. Professor Berendt, who was the rapporteur for this session, has additional useful thoughts based on her own experience: 'Users' contexts and ways of learning would have to be taken seriously. Such training forms, and of course the good security and privacy practices they are meant to create or sustain, cost time and resources, and people cannot reasonably be expected to do this on the side in addition to all their other tasks. Managers, teachers, etc. thus need to commit more deeply than . just giving lecture-style instructions, also questioning their own practices. Trade-offs (e.g. with costs, labour, flexibility, hierarchy) will need to be taken into account, and organisations will have to confront and address the conflicts that can arise between different stakeholders, user roles, etc. This non-uniqueness of the notions of security and privacy will probably be among the most challenging, but also most interesting, aspects of future education and training.

2.2 Austrian competition

Austria's search for cybersecurity talent ([9])

Cyber Security Austria (CSA) organises an annual contest in cooperation with the Ministry of Defence and Sport. Cyber Security Challenge 2014 is be the largest such contest in the search for the country's most promising young hackers, to secure their talents in the long term and to help them develop into cybersecurity experts of the future. 'With Cyber Security Challenge 2014, we want to strengthen the image of the talented local hacker scene due to the first cybersecurity challenge', says Joe Pichlmayr, council member for Cyber Security Austria (CSA). 'We are searching hard for Austria's young and up-and-coming IT talent who want to prove their skills in a legal way and want to compare their knowledge with others in their age group.'

Last year over 600 teenagers participated. This year, a big increase in the number of contestants is expected as the criteria have been extended to cover university students as the challenge goes into its third year. Additionally, the potential winner has increased motivation: a place in an international competition against winners from Germany and Switzerland — the international Cyber Security Challenge — who will challenge Austria's finest in the grand finals.

Searching for 'insanely good' talent

With the slogan '**Are you insanely good? Then show us!**', CSA, the Ministry of Defence and Sport and Kuratorium Sicheres Österreich (KSÖ) are inviting all pupils and students in the country to get involved with IT security.

'For us this contest is not only about finding the best young hacker in Austria: we also want to understand how far advanced the skills and knowledge of the young people already are,' says Joe Pichlmayr. 'Therefore, we are especially interested in their paths to finding solutions and how they think, act and process ways to solve various hacks.'

Interested teenagers can register for Cyber Security Challenge Austria 2014 on the official website ([10]). The challenge commenced on 6 May 2014. The Hacking Lab — a special kind of Internet security laboratory — was unlocked on the first day, and it is on that platform that the challenge is taking place.

'Hacking Lab' as the centrepiece of the challenge

The centrepiece of the challenge is the so-called Hacking Lab. This refers to a remotely controlled security laboratory, which was developed by Compass Security AG. The laboratory contains 150 different security challenges from all areas of IT, which can be used in the context of the security challenge. To solve them, the contestants access specifically prepared, vulnerable systems through a VPN remote connection. Another feature of the Hacking Lab is the option to link tasks with solution applications, discussion possibilities and scoring.

A challenge for ambitious young hackers

School pupils, young people and students

The tasks are very diverse, requiring pupils and students to successfully pass one or more technical tests in order to finish the challenge. The solutions are then submitted online to the Hacking Lab. During the submission, additional questions are posed, such as which IT security breaches were available, how the security breach could be used and what was the best alternative to protect the system from these threats.

([9]) For further details contact joe.pichlmayr@cybersecurityaustria.at

([10]) http://www.verbotengut.at

'The Cyber Security Challenge has clear ambitions to educate contestants. It is important for us that the young people do not only encounter matters of hacking and IT attacks, but must also address and understand counter-measures. With this action, we want these talented people to have a certain perspective on the matter, similar to those of IT security experts,' Joe Pichlmayr says.

How the Cyber Security Challenge works

On the start date on 6 May, all participants received new assignments which are to be solved alone and creatively. Experts from Cyber Security Austria are conducting ongoing supervision and performance evaluation, and supporting the contestants as coaches.

The best 10 participants in each of the contests, for school pupils and young people and for students, qualify for the national finals, which were held from 11 to 14 September 2014 in Hagenberg.

The two winning teams of pupils and students then represent Team Austria in the international Cyber Security Challenge. They challenge the winners of the equivalent German and Swiss challenges at a contest which took place from 3 to 5 November 2014 in Fürstenfeld, during the largest Austrian security event, the ICT security conference of the Ministry of Defence and Sport.

Live hacks, finals and appealing prices

The finals took the form of a team competition, where two teams with five people in each have to compete against each other in different live challenges. The awards ceremony of the Austrian challenge took place on 13 September 2014 at the Ars Electronica Centre, Linz. The awards ceremony for the European Cyber Security Challenge 2014 was on 6 November 2014 in the festivities of the Museum of Military History (Heeresgeschichtliches Museum) in Vienna in the presence of politicians, economists and representatives of government bodies.

'Hire the hackers' — cybersecurity experts for public authorities and businesses

Beside Cyber Security Austria, the Defence Agency and the Kuratorium Sicheres Österreich (KSÖ) are also supporting Cyber Security Challenge Austria 2014 and thereby bringing it to the attention of authorities and businesses.

The Austrian job market is urgently seeking highly qualified IT security experts. The protection of essential IT infrastructure is becoming more and more important in both the public and private sectors. To meet this challenge on a long-term basis, young people with talent and enthusiasm for IT must be encouraged from the earliest age possible and trained to be the future IT security specialists that the region needs.

'For the ÖBH (Army of Austria) to fulfil its goals, it needs a secure and reliable operation with various ICT systems,' explains ObstdG Mag. Unger, head of the department for cyberdefence and ICT security. 'Furthermore, the ÖBH has [been given] responsibility for cyberdefence. That is why it needs a large number of highly qualified ICT security experts — firstly, to protect the military ICT systems and secondly, to help in the cybersecurity area if others cannot continue anymore.' Therefore the CSA, the Defence Agency and the KSÖ are following the approach of 'hiring the hackers'. Young IT talents need to be scouted at an early age and their skills and strengths need to be developed with the support of public authorities and businesses. 'Together with the experts from Cyber Security Austria, we want to establish the crucial job sector of IT security [among young people] to make Austria more secure,' adds Kunstmann. 'The economy knows of its role and responsibility and supports the challenge on an organisational and financial level.'

Preventing illegal activities

For the CSA the challenge also has other goals. 'Through a direct and early approach to youngsters who are passionate about IT, we want to prevent from them using their knowledge sooner or later for illegal activities. With the challenge, we set a certain representation in the group of young adults and deliberately want to encourage them to follow a legal path.' Participants in Cyber Security Challenge Austria have to sign a code of ethics, whereby they confirm in writing that they have been informed about the legal boundaries of hacking, and that they are not allowed to use the techniques they have learned for abusive purposes.

Widespread support from politicians, economists and government

For Cyber Security Challenge Austria 2014 to meet its goals, the organisers rely on cooperation with the Ministry for Internal Affairs and the Ministry for Defence and Sport. The Office of the Chancellor, ENISA and the Federal Agency for IT have also provided support. Financial aid from notable companies in the sector is also greatly appreciated. Special thanks go to A1 Telekom Austria, Sprecher-Automation, Philippeit, FabaSoft, Kapsch, ACP, SEC-Consult, IKARUS, Symantec, ArrowECS, Barracuda, the Computer Company Computershop GesmbH, the WKO — Bundeswirtschaftskammer, A-Trust and the Bundesrechenzentrum BRZ as well as the University of Applied Science Upper Austria, the University of Applied Science Technikum Vienna and the University of Applied Science St Pölten.

Several insights from the Cyber Security Challenge Austria 2012/13

The Cyber Security Challenge 2012/13 gave the organisers many surprising insights and featured many more 'wow moments' than expected. Over 400 pupils and young people took part in the first challenge, which was conducted through the virtual laboratory environment of the Swiss Compass Verlag (Hacking Lab). Their performances surprised both the organisers and operators of the hacking labs. In certain exercises, the solution rate was 10 times higher than for other, comparable participants who had taken part in the hacking lab. In addition, more contestants than expected successfully accomplished the hardest tasks available.

> The exceptionally high performance level was later confirmed by the participation of the finalists of the Cyber Security Challenge in other 'hacker contests' with a very high ranking.

The 25 best contestants in the challenge and Cyber Security Austria enjoy a constant dialogue, which was formed through the Centre of Excellence. In the Centre of Excellence, it has been ascertained that the participants know very well what is allowed and what is prohibited. They want to distance themselves from illegal 'hacks'.

Most of them suffer from the fact that their family and school environment cannot recognise, appreciate and value their performance and skills — a well-known phenomenon that many very gifted people have to tolerate. Every one of the top 10 in the challenge can choose from numerous offers from the business world by this time. Immediately after the contest and awards ceremony, the finalists received several job offers. In the 2013 challenge, the group of participants was extended from school pupils and young people to students from universities of applied science and other universities. The best of the best are determined in two parallel contests and will confront the winners of the Swiss challenge after the finals. For Cyber Security Austria it is clear that the challenge needs to be expanded and to establish itself as a 'high-class-event'. Therefore the bilateral competition with the Swiss will only be a first step in the right direction. It will also support awareness for the construction of the structures that are needed to motivate and develop highly talented top people.

Further information on Cyber Security Austria ([11])

About the Agency of Defence

The Agency of Defence is an intelligence service of the Austrian army with three main tasks — the classic task of intelligence protection, the perception of military security including ICT security and the perception of tasks in line with Information Security Law — as well as the ability and competence to recognise threats to military security in time for them to react with proper counter measures. With the establishment of military computer emergency readiness teams (MilCERT), Austria has taken a major step towards a general concept of defence against digital threats. These capabilities (in cooperation with other departments in the Austrian army) complement special knowledge in the areas of forensics or the audits of rooms and facilities.

2.3 Swiss competition

The Swiss Cyber Storm association organised the 2014 edition of its annual Cyber Security Challenge. This was the largest contest in the search for the country's most promising young cybersecurity talents, to promote their skills and to convince them to pursue a career in cybersecurity. In 2013, over 200 contestants participated. A slight increase in contestants was registered in 2014, as the participant criteria have been modified to include people who have completed their bachelor's degree — but do not hold a higher degree — and are no older than 30 years. Furthermore, the fact that the international competition in which the winning team can participate has been extended from two to three countries (the others are Austria and Germany) should make the challenge more attractive.

Basic idea and target audience

The challenge is very diverse in that pupils and students have to successfully pass one or more technical tasks in order to finish it. The solutions are then submitted online to a Hacking Lab. A solution consists not only of how the problem was solved but also how the underlying weakness in the software/hardware/system architecture or similar (if any) would have to be modified to fix or prevent it. By requiring this additional step, Swiss Cyber Storm stresses its ambitions to educate contestants.

Swiss Cyber Storm wants young people not only to be met with matters of hacking and IT attacks, but also to learn to address and understand counter-measures.

Hacking Lab: providing a platform for cybersecurity challenges

The centrepiece of the challenge is the 'Hacking Lab' — an online platform offering a controlled security laboratory developed by Compass Security AG. The laboratory offers free access to a limited set of security challenges, for example those published by OWASP, but it can also be used to

[11] http://www.cybersecurity.at

establish public and private security challenges or to do security training. To solve the challenges, the contestants usually download a live CD or virtual machine image (e.g. for VMWare). Both of these come with all the required tools pre-installed and offer a one-click solution to initiate the VPN connection to the security laboratory from where the specifically prepared systems for the challenges are accessible. However, some of the challenges can also be solved locally. For challenge organisers, the Hacking Lab offers convenient management and teacher views which make things like rating submissions and providing feedback to the contestants easy. The Hacking Lab platform is basically open to anyone. It attracts a large community of people from all over, some of whom even actively propose and create new security challenges. Currently, there are over 150 security challenges in domains like web application security, forensics, malware analysis, cryptography, mobile device security, operating systems security and reverse engineering. Compass Security AG says it is also very open to academic partners: it cooperates, for example, with the universities of applied sciences in Zurich (ZHAW) and Bern (BFH).

Organisation and support

The Swiss Cyber Storm Security Challenge is organised by a committee consisting of members of the Swiss Cyber Storm association and works on an unsalaried basis. In 2014, the Swiss government is supporting this effort with patronage from the Swiss Reporting and Analysis Centre for Information Assurance (Melani) ([12]) and the Swiss Police ICT association ([13]) (German and French only). This association sponsors the annual Swiss police computer science congress, SPIK, whose goal is to make all involved specialists and managers of police forces, the IT industry and politicians familiar with new ideas, developments and products. A political committee with representatives from the five governing parties, a civil servant and a police commander serves as a consultative body and a link to politics. The patronage and support from the government (Melani) and organisations like Swiss Police ICT is crucial for finding sponsors — which is vital since there is (almost) no financial support from the patrons — and for the promotion of the challenge. However, Swiss Cyber Storm has demonstrated that even without financial support from the government, it is possible to organise and run such a challenge. Special thanks go to supporting companies like Aspectra, InfoGuard, Kaspersky, Kudelsky Security, PwC, Swisscom, Symantec, terreActive, United Security Providers and the two universities of applied sciences in Zurich and Bern. It is important to note that Swiss Cyber Storm was inspired by the Cyber Security Austria team and has strong ties to it. It is also important to note that, for 2015, there are ongoing negotiations with the Federal Department of Foreign Affairs (EDA) to bring the challenge up to the next level by providing additional financial and organisational support.

How the Cyber Security Challenge works

The challenge is split into three phases.

Phase 1	Registration and online qualification ([14])	May to September
Phase 2	Swiss national final	21–22 October
Phase 3	European Cyber Security Challenge	3—6 November

([12]) http://www.melani.admin.ch/index.html?lang=en
([13]) http://www.spik.ch/
([14]) Using https://www.hacking-lab.com/index.html

Phase 1: Registration and online qualification

In the first phase, pupils and apprentices between 14 and 20 years old and 'cyber talents' between 20 and 30 years who do not (yet) have a master's degree ([15]) can register for the Swiss Cyber Storm qualification event on the Hacking Lab platform. Participants in this event have access to the security challenges, which get unlocked on a monthly basis between May and September. By solving these challenges, which include tasks from domains such as web application security, cryptography, forensics, penetration testing or reverse engineering, they can collect points to improve their ranking among the participants. Checking and rating the solutions submitted by the participants is the most time-consuming and expensive task for the organiser. Since most challenges can be solved in many different and sometimes unforeseen ways, the submissions must be checked and rated by IT security experts. This expertise is also required because the solution does not only have to include a description of the solution to the challenge (e.g. finding and exploiting a vulnerability in a web application) but also a description of how to mitigate the problem.

Phase 2: Swiss national final

After the end of the qualification phase, the top 10 participants from each of the two categories were invited to the Swiss national final on 21 and 22 October 2014 in Lucerne. On the first day, the two teams for the next day's final, consisting of five contestants from each of the two categories, were formed. Team-building activities were planned and supervised by two experts. In the evening, the contestants participated in the VIP event of the Swiss Cyber Storm IT security conference. During this event, the contestants had the opportunity to talk to speakers, IT security professionals and decision-makers to extend their network and to ask critical questions or to discuss fresh ideas and viewpoints with the 'establishment'. The awards ceremony of the Swiss Cyber Storm cybersecurity challenge was held the next day during the closing session of the Swiss Cyber Storm IT security conference running in parallel to the Swiss national final.

Phase 3: European Cyber Security Challenge

The winning team then represented Switzerland in the European Cyber Security Challenge from 3 to 5 November 2014 in Fürstenfeld. The finals took the form of a competition between teams from Austria, Germany and Switzerland, who compete against each other in different live challenges. The Swiss delegation consisted of the Swiss team and seven staff members from the Swiss Cyber Storm association. After the challenge, the teams traveled to an awards ceremony on 6 November at the Museum of Military History in Vienna, in the presence of politicians, economists and representatives of government bodies.

Need for cybersecurity experts for public authorities and businesses

The protection of essential IT infrastructure is becoming increasingly important in both the public and private sectors. The Swiss job market is desperately seeking highly qualified IT security experts and to ensure this on a long-term basis talented young people who are enthusiastic about IT must be encouraged from the earliest age possible, and trained to become the future IT security specialists that the region needs. However, this is not easy because there are so many 'cool' opportunities in IT which are much more visible to young talents than a career in IT security. To improve the odds, IT security must be made more visible and tangible. Swiss Cyber Storm and its supporters are convinced that an (inter)national IT security challenge is an important building block in achieving this goal. With its supporters ranging from the Swiss Reporting and Analysis Centre for Information Assurance (Melani) and the Swiss Police ICT association to sponsors from the private sector, Swiss

[15] For details see https://www.swisscyberstorm.com/securitychallenge/eligibility-requirements/

Cyber Storm is making sure that the interests and concerns of authorities and businesses are respected and taken into account.

Preventing illegal activities

For most youngsters, learning how to hack systems is more appealing than learning how to protect them. Through a direct and early approach to young people who are passionate about IT, Swiss Cyber Storm wants to prevent them from using their knowledge, sooner or later, for illegal activities. With the challenge, these youngsters not only get an opportunity to test their skills in a legal setting but they are also encouraged to follow a legal path. Participants in the Swiss Cyber Storm Security Challenge have to sign a code of ethics, where they confirm, in writing, that they have been informed of the legal boundaries of hacking and that they are not allowed to use the techniques they have learned for abusive purposes.

2.4 Romanian competition

There is one important rule though — hack before getting hacked!

DefCamp (D-CTF) in numbers

- In 3 years, four editions with teams of maximum five members
- Jeopardy, attack/defence and cyberattack scenarios
- 800 teams worldwide (75 % of the total number of teams competed in 2013)

How it all started

D-CTF was born in 2011 together with DefCamp, one of the most important conferences on hacking and information security in central and eastern Europe. The goal was to bring about hands-on talks about latest research and practices from the information and security field, gathering under the same roof security specialists, entrepreneurs and academics, from both the private and public sectors. But a simple conference was too easy and so they created D-CTF. The operation started in 2011 with around 10 teams and has registered about 800 teams worldwide to date (75 % of the total number of teams competed in 2013).

Why D-CTF?

D-CTF says it's all about teamwork, having one's eyes wide open and possessing remarkable skills. It spreads the newest security techniques and enables the security skills of the teams to be measured. A complete team covering all the main skills is always the best option for getting into the finals. At the same time the competition strengthens both technical and management skills; the leader coordinates every step of the process, making sure that the team is following a line that will result in capturing the flag. Mystery, mathematics and complicated algorithms combine to make everything even more challenging. Some consider this competition to be a game, because originally it was a game that simulates small team combat, based on defending an immobile flag while trying to capture the flag of the other team.

Having the right team and knowing the right techniques to achieve the goal is most important. Of course everything is doubled by:

- effectiveness;
- responsiveness;
- team coordination.

How it works

D-CTF has two main parts: online qualification followed by a final challenge that usually happens during DefCamp. The essentials regarding the online qualification are that the team leader registers the team and it waits for the challenges to be sent on a specific day announced on the official website. The team then has 48 hours to solve 25 problems in jeopardy style. The 10 teams that finish all the challenges in time with the best results can enter the D-CTF finals that happen during DefCamp. In the finals, the teams will have another 24 hours of challenges. The best teams will receive prizes in the form of both cash and products worth thousands of euros.

Rules to follow:

- Teams can have a maximum of five members (including the team leader).
- Denial of D-CTF service/servers is not allowed.
- Finding bugs in D-CTF infrastructure can give the team more points.
- The most important rule is though — hack before getting hacked!

Results:

- 48 hours of intensive work
- Gaining knowledge
- Simulating a live experiment
- Facing challenges
- Cash and/or an awesome experience

D-CTF says: ‘It’s an addictive competition that always manages to bring the strongest, [most] skilled and [most] passionate teams that are at any time ready to take over the world, to face the challenges and of course to take all the money — the cash prizes.’

Why D-CTF?

The Cyber Security Research Centre from Romania (CCSIR) ([16]) is a non-governmental organisation with the sole purpose of promoting, supporting, implementing and coordinating security research in the information security field in Romania, as well as international actions with short-, medium- and long-term partnerships in the information security arena. ‘We are a team of passionate people with a technical background,’ CCSIR says, ‘and now our main goal is to spread respect for cybersecurity competitions worldwide.’

Organisation and support

‘We struggle every year to get sponsors supporting our initiatives,’ CCSIR says. ‘In 2014 we’ve created a special package in order to get a specific amount of money for D-CTF because we believe that it’s the most important asset we have. Also because we have skilled people registering for this

([16]) http://ccsir.org/

competition and we want to reward and motivate them to further develop their skills and to keep their eyes wide open for challenges. We put a lot of work every year into developing and spreading the word about D-CTF and every year more and more companies are interested [in providing support] either for hiring talent or to help the organisation to achieve the annual goal.'

The D-CTF success story

'It's great to see talented teams going further after D-CTF finals,' CCSIR adds. 'Hexcellents, the 2012 and 2013 winning team from D-CTF, is the team that represents Romania in the largest CTF competitions worldwide. Not only this, but [it] also ranked in the top 15 out of almost 1 000 teams from all over the world. Also, one of our amazing challenges developer has won several international competitions [and] he is now in one of the top five international teams for CTFs and he was recruited by Facebook.'

The prizes

2.5 Spanish competition

CYBERCAMP[17]

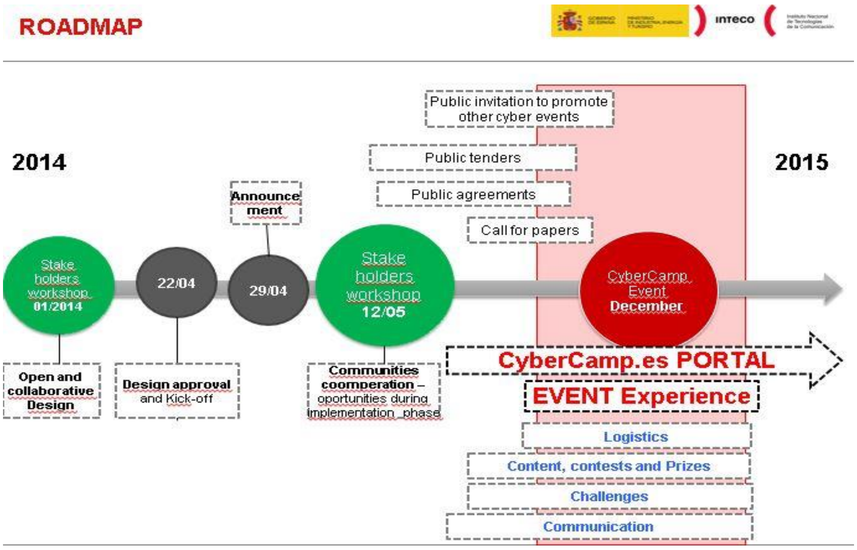
The aim of Spanish CyberCamp is to promote cyberskills talent of our future professionals in cybersecurity by running advanced challenges and competitions for best spanish students and researchers in cybersecurity as well as best international talented professionals.

CyberCamp is sponsored by the government through the Confidence Plan[18] of the Digital Agenda of Spain[19].

The first edition has an online qualifying phase during October-November 2014 and the physical event takes place during a weekend on 5-7 December in Madrid.

The physical event is a great opportunity to share experiences among the different participants and to create a better link between the top talents or best projects to the industry recruiters or investors' interests respectively.

- Incentives and prices for the best contesters: networking, entertainment, recruiting, grants, attractive training and travelling to international events;
- Challenges: top talents from previous online phase are invited to the event to compete at CyberCamp (CTF- Blue Team/Red Team contest). Final composed of advanced challenges and cyber-exercices with limited time;
- Practical Training, Labs, key notes, hackathons, conferences, round tables, practical workshops, demonstrations of prototypes, project ideas, elevator pitches, entrepreneurs' success cases, speed dating with BAs, recruiting space for enterprises by using score cards, etc;
- Public space: used in cultural events, relaxing atmosphere.
- Production and logistics: entertaining activities, catering, hostesses, translation, registration, accommodation camp, audio-video media, etc;


ROADMAP
inteco
2014
2015
Stake holders workshop 01/2014
22/04
29/04
Announce ment
Stake holders workshop 12/05
CyberCamp Event December
Open and collaborative Design
Design approval and Kick-off
Communities coomperation – oportunities during implementation phase
Public invitation to promote other cyber events
Public tenders
Public agreements
Call for papers
CyberCamp.es PORTAL
EVENT Experience
Logistics
Content, contests and Prizes
Challenges
Communication

[17] More information check http://cybercamp.es or contact Ignacio Caño Luna / Raúl Riesco- INTECO Spain

[18] http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaconfianza/2.%20Material%20complementario/PlanDetallado-ADpE-5_Confianza.pdf

[19] http://www.agendadigital.gob.es/digital-agenda/Paginas/digital-agenda-spain.aspx

Experts and key communities

CyberCamp tries to identify the best talent and expertise and have the support of key communities of the Internet. Cybercamp is open to scientific, university, company, online communities or students who want to use it as a platform to disseminate their projects.

Currently, there is a contact network with international universities, public and private institutions in the field of science, innovation and entrepreneurship that we will consider accordingly. Likewise, many online communities and youth associations that support dissemination of Cybersecurity activities.

All this makes a comprehensive approach so that CyberCamp can consider the different needs to be met before and during the Event.

In addition, partners and potential sponsors are supported in a specific communication strategy. It gives opportunity to brand visibility and improving corporate image. Clear objectives are being defined to align the audience Cybercamp and interested brands.

Interactive support platform

CyberCamp wishes to broadcast the event activities and encourage conversation among attendees. The platform will be a place to collect all content, materials and discussions that occur during the event.

The platform is designed exclusively to meet the needs that can generate the call for a challenge, both locally and globally. It allows users to register on the challenges that interest them and can upload their projects and provide all necessary documentation. It bridges talent, companies and institutions to create value and contribute to innovative solutions and ideas.

The platform may also collect data to participate in itineraries such as "the best entrepreneur" contest. The information received will be considered for selection, evaluation and development of participants to raise Cybersecurity talent in Spain.

The cyber security challenge is split in two phases:

Phase 1	**Online Challenge** - Registration and online qualification www.cybercamp.es	October
Phase 2	**Insitu Challenge** - Spanish national final	6-7 December

Phase 1: Online Challenge - Registration and online Qualification

CyberCamp.es portal was open for registration from September.

It allowed the users to assess their skills during a first qualification phase. Different categories were released every week in October for the contest. After that, the challenges remained active as a playground outside the contest. Quick responses were rated higher for each of the challenges and bonus decrease over time. The first to answer correctly has 200% value of its original score, the second answer has 150%, the third 125% rating and, after that, correct answers are valued at 100%.

Type of online challenges:

- System Vulnerabilities: related with virtual images analysis and vulnerable configurations.
- Reversing: related to Analysis of malware and APKs.
- Forensics: Memory Dumps and USB / HD disk.

- Code Analysis: source code review for potential vulnerabilities
- Web Vulnerabilities: attacks to websites.
- Cryptography: Analysis of Steganography and ciphering.

Phase 2: In situ Challenge - Spanish national final

It is held in Madrid during Cybercamp Event on 5-7 December. The final phase of the challenge is the so-called “Insitu Challenge”. It refers to a fortified platform for cybersecurity challenges as a controlled security laboratory.

A platform allows the assessment of expertise and users reaction in an unknown environment. The challenges will be available in Spanish and English with an educational focus and the aim is to develop their technical skills. The simulation environment is similar to a real case where participants use their own desktop equipment to perform quizzes. The platform has a web interface that allows access from the most common operating systems.

The design allows the grouping of tests in the following categories or phases:

- Recognition: Phase where participants test their ability to detect vulnerabilities in exposed environments.
- Raid: This phase offer systems to try to access them.
- Discovery: In this phase is focused on the internal network infrastructure system that was attacked.
- Capture: this phase evidences guide the participant to gain control over critical systems in the attacked environment.
- Exfiltration: During this last phase, the participant obtains critical system information and take it to its computer.

The estimated challenge duration is 6 hours. We are selecting the number of suitable tests, duration of each test with certain specifications, test complexity, dependencies between tests, objectives to be achieved and other design elements.

2.6 United Kingdom competition

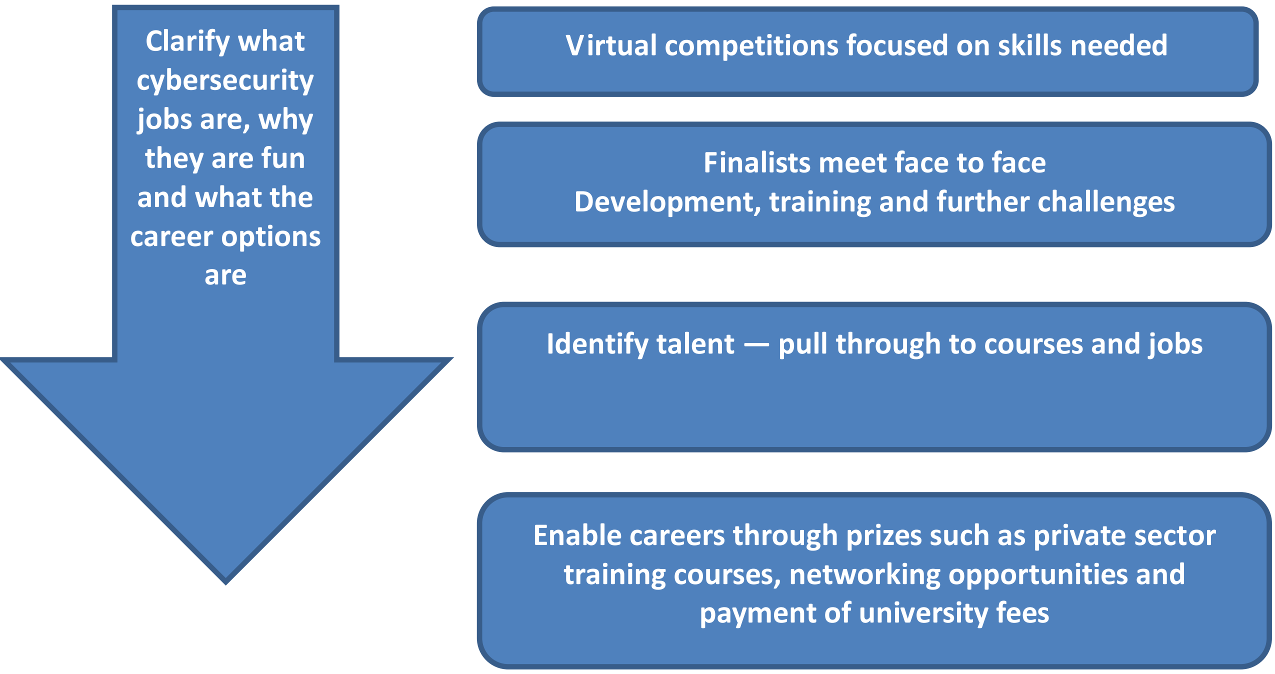
Cyber Security Challenge UK Ltd is a not-for-profit company formed in March 2010 to plug the cybersecurity skills gap in the UK. About 90 % of professionals surveyed had difficulties recruiting the cybersecurity talent needed by their companies, across all eight categories of cybersecurity jobs surveyed. Nearly 60 % predicted (correctly) an increase in the number of jobs there would be in the British market in cybersecurity. The mission of the Cyber Security Challenge is to ensure that sufficient numbers of those, of any age, with a talent for cybersecurity are identified, inspired and enabled to find training and fill such jobs as are needed to provide efficient protection of the United Kingdom’s economic prosperity, national security and chosen way of life. The company runs on sponsorship from the government, the private sector and academia, all of which recognise the national importance of cybersecurity, not just for national security reasons or to allow citizens to safely choose to take actions using digital means but also to underpin the economy and enable the market growth needed for the United Kingdom’s future prosperity and success. Cyber Security Challenge is a unique programme of activities designed to introduce sufficient numbers of talented people to learning and career opportunities in the cybersecurity profession.

> *At the heart of this is the national competition programme but a growing schools programme, learning opportunities at cybercamps and networking initiatives are all linked together to identify, inspire, inform and enable more EU citizens resident in the UK to become cybersecurity professionals.*

Only those not currently working in cybersecurity are eligible to compete in these competitions. Previous winners have ranged from a postman who now works for Royal Mail as a vulnerability manager to a university undergraduate also now employed in a cybersecurity profession. Cybersecurity skills shortages are a problem in many countries. In line with British government support for international collaboration on cybersecurity issues, the Cyber Security Challenge welcomes partnerships with other organisations which do similar work in Europe or elsewhere. Its sponsors are often multinational and there is interest amongst them in supporting competitions run in other countries and in getting value from the potential public relations opportunities and benefits of such competitions. This could be by many countries playing the same competition or a play-off between teams from different countries. An objective in Cyber Security Challenge UK’s business plan for 2014 is ‘to forge partnerships with other competition runners to link to more people interested in cybersecurity and encourage our candidates to experience other competitions’.

Competition programme

The initial concept was to identify talent through a range of virtual competitions (to reach large numbers), then to meet the most talented at face-to-face sessions and finally to enable them to get jobs, through giving them prizes that provide training and networking opportunities.



Clarify what cybersecurity jobs are, why they are fun and what the career options are

Virtual competitions focused on skills needed

Finalists meet face to face
Development, training and further challenges

Identify talent — pull through to courses and jobs

Enable careers through prizes such as private sector training courses, networking opportunities and payment of university fees

The company was registered in March 2010, launched in April and started its first three competitions in July. Only one, designed by QinetiQ, was a new competition: Sans Institute provided a challenge it had used in the United States. The US Department of Defence allowed Cyber Security Challenge UK to be a strand of its international digital forensics competition. Each of the three competitions dealt with a different subject within cybersecurity and the winners flowed through to one of two face-to-face competitions and then a masterclass final. Within 3 weeks 4 000 people had registered to play.

Cyber Security Challenge UK now runs many more competitions but sponsors continue to supply all of them as part of their sponsorship contribution. The Cyber Security Challenge team moderates for quality and fairness and ensures competitions are testing the skills that businesses and government need. It manages the marking of face-to-face competitions with the help of sponsors from different companies who observe candidates' performance, scoring them on a matrix of skills and competencies. The types of competitions run have tested defensive skills, knowledge of different vectors of attack, digital forensics, policy and procedures and more.

The virtual nature of the first games allows large numbers to play but only 100–200 are successful in reaching the face-to-face stage and this year there were 40 at the masterclass final. Some candidates do not make it to the final as they get jobs in cybersecurity, rendering them ineligible. Cyber Security Challenge UK has built on the success of its first year and developed year by year. There are now about seven virtual challenges annually. Its most recent virtual competition, written by Sophos, had over 600 registrations. Then there are about four face-to-face challenges, with some 30 candidates in each. The plan for this year is to establish a play-on-demand platform which will allow candidates to play at different times and should increase the breadth of the company's reach. In addition it runs ad hoc competitions like a Christmas cipher which had some 1 500 entrants.

Technical competence is the key component but at the face-to-face stage interpersonal skills are also tested. The masterclass winner, the cybersecurity champion of the United Kingdom, will be strong in both technical and interpersonal skills. There is not just one winner and a runner-up though. The prize portfolio (all donations of training or networking opportunities from companies, government or universities) is worth about GBP 100 000 so a lot of candidates benefit and get the lift they need to make a successful start in a career in cybersecurity. Candidates in each masterclass are marked both for their individual performance and as part of a team.

The last masterclass had teams being the front-line defenders in dealing with a series of attacks. In the course of a day and a half the attacks emerged as being not just criminal but nationally critical, bringing down national infrastructure. The teams had to identify what was happening technically, find ways to stop the attacks and also brief the press and government. This competition was written by BT, GCHQ, the National Crime Agency and Juniper Networks. Candidates had an exhausting but exhilarating time, learning much along the way. The markers came from about 20 different sponsor companies. For the first time all the competitions in this year's annual programme are linked around a single theme. This is to raise excitement and fun as the programme develops and give a feeling of progress as the story unfolds. The last masterclass awards ceremony was interrupted by a video from a masked group calling themselves the Flag Day Associates whose terrifying messages warned of future attacks on the United Kingdom. Following this, the challenge announced that the investigation of, and defence against, the threat posed by the Flag Day Associates will be undertaken by the challenge's candidates. In order to best defend the United Kingdom from this threat, the competition programme over the coming months will serve to both find out more information about this mysterious organisation, and identify the skills and expertise required to protect against it.

Issues and candidate stakeholder groups. Knowledge of training and jobs

Cyber Security Challenge UK says that one first year surprise was that most of the candidates (who by definition were interested in cybersecurity) stated in a questionnaire that they knew little or nothing about cybersecurity careers and training opportunities. However 84 % were interested in being introduced to potential employers. Most were competing to demonstrate their skills, not to find a job. But by the end of the year 87 % said they were more likely to consider a job in cybersecurity and over 90 % thought they had learned more about cybersecurity jobs and developed their skills. 'In retrospect it is not surprising that people are not knowledgeable about cybersecurity jobs which are quite new and totally different from the security jobs of a decade ago,' the company says. 'In addition our education system has not yet grown to include cybersecurity within the curriculum at schools.'

> *We realised that we needed to do more than spot available talent, it is necessary to develop a whole pipeline of people for the future.*

In response to the need to provide information about jobs, the company is continuing to develop the opportunities for candidates to network with employers, especially its sponsors, attend cybersecurity events, run cyberfairs and build the provision of careers and training information on its website. Candidates have found that meeting sponsors has been important and has brought the jobs to life for them. To build the pipeline for the future the company is engaging with different stakeholder groups from those at school or university to those already employed, but not in cybersecurity.

One candidate recruited by a PwC threat and vulnerability team commented: ‘The challenge helped me to meet employers who could see what I could do.’

Development

All competitions give some opportunity for development and learning. Cyber Security Challenge UK says it welcomes the fact that candidates can research answers for some of the virtual competitions. It is working to grow the opportunities to develop and learn and is establishing a more structured sort of cybercamp. It has already run cybercamps hosted by universities and by the UK Ministry of Defence and in 2014 is running two cybercamps with a new design aimed at those who know they want to follow a cybersecurity career. These will pilot a structured programme of learning and competitions and those who reach the required standard will qualify to take a government-recognised qualification, to equip them for jobs. Introductory training materials will also be provided online to equip more people to compete.

Diversity

Only 8 % of year one candidates were female and only 4 % of year two. There have never been more than two women at a masterclass. The United Kingdom is keen to recruit from the whole population and it is a government objective to draw more women into technical jobs. Cyber Security Challenge UK is working with partners like Stemnet to maximise impact and has launched a number of initiatives designed to involve more women in competitions. These range from showing successful women as role models in video clips about jobs on the website to reshaping some of the marketing materials and running an event to draw in the support of the current female cybersecurity community. The latter took place at Bletchley Park and some of the original female code-breakers attended. Their role in successful wartime code-breaking is only now being recognised. *The Times* newspaper reported this message from one of the original code-breakers, Ruth Bourne, now aged 87: ‘It is all about brains, brains, brains … Don’t be put off by the mathematical suggestions. If I could be trained to operate one of those machines as a kid … you could do it now in spades.’

Schools

Cyber Security Challenge UK says it wants to reach anyone of any age who might have the talent to do well in cybersecurity. Each year the standard of its candidates has got higher. ‘This has been good for employers wishing to recruit but it has meant that few schoolchildren reach the face-to-face stage of our competitions and we want to avoid discouraging them. In response to this a schools programme was launched last year initially reaching over 500 schools. This is growing and in 2014/15 will reach classes of about 30 in over 1 000 schools.’ The programme has two strands — firstly, a teacher pack giving a lesson plan keyed to the small relevant items in the national curriculum and a number of exercises designed by sponsors, and secondly, a competition, focused this year on coding. The six best schools in the coding competition competed in a face-to-face final which demonstrated the physical impacts of cybersecurity — carrying out, for example, actions to move a robot. The enthusiasm generated has been encouraging and school groups have participated in some of the networking events involving key people in cybersecurity. The government is seeking to introduce some cybersecurity into the curriculum and Cyber Security Challenge UK says it will develop its programme to link into this and continue to support teachers. ‘We are working with one of our sponsors, Northrop Grumman, to introduce the Cyber Centurion programme to the United Kingdom (Cyber Patriot in the United States). This will plug the gap between our schools programme and the national competition programme, drawing students through from one to the other.’

Universities

Cyber Security Challenge UK is working with some universities which are developing their own competitions and playing against other universities. The company would like to further develop its work with universities (perhaps through university interest groups to foster enthusiasm for jobs and cybersecurity as a subject), run university competitions and draw good candidates through to the national competition programme. Cybersecurity skills may be found not only amongst those taking IT or computer studies but a wide variety of other subjects. Cybersecurity is becoming a life skill needed by all and we would like to encourage modules on cybersecurity in a number of subjects, the more obvious being engineering and business studies.

People already in employment

Those already in jobs but lacking the means to prove their competence and transition to cyberjobs are low-hanging fruit for those looking to recruit. They may prove to be the group which will benefit most from the learning opportunities that the new cybercamps will provide (see above).

Alumni

Cyber Security Challenge UK has a database of around 11 000 individuals interested in cybersecurity and successful candidates become members of an alumni group. This group supports the company in a number of ways, including providing outreach to new communities, informing its activities and sometimes helping with the running of competitions.

Sponsors: why do they offer support?

Private sector sponsors are attracted firstly because they recognise the skills shortage in cybersecurity. They see this as a problem that will impact on their businesses and that they cannot rectify alone. So corporate social responsibility is a starting block: beyond this, they look to benefit in different ways from their partnership with the challenge, reaching agreements that give different benefits to both parties. The main benefits to companies are: recruitment opportunities; PR marketing and publicity, showing the company's excellence in cybersecurity; networking opportunities through meeting senior staff from other companies — including through the competition — government and academia; opportunities to display thought leadership; a way to demonstrate support of the government strategy; and showcasing training provision. The main benefits to the challenge are a balance of finance to run the business and value in kind, which varies from developing and running a competition to hosting the Cyber Security Challenge UK website or hosting one of its networking events. The platinum sponsors form an advisory board that advises the Cyber Security Challenge Board on the development of the business.

Government sponsors the challenge for many of the same reasons as the private sector. It recruits from amongst its candidates. The British government's cybersecurity strategy has a strong emphasis on developing cybersecurity skills and capability and names Cyber Security Challenge as one of the ways of helping to fill the cybersecurity skills gap. It also recognises that its activities support other government cyberobjectives like raising security awareness.

Academia is developing more courses that include or are centred on cybersecurity and is working with business and government. Academics have also welcomed links to their local business communities.

'SMEs are under attack from hackers, but where do you go to ensure that you are more secure? There is a massive shortage of new recruits to the cybermarket. The potential recruits are there, and often in unrelated roles such as heating engineers and postmen. The challenge is to find them, train them and bring them into the cyber workplace. By sponsoring the Cyber Security Challenge you can ensure that such potential recruits are identified and given a chance. In this way you help to fill the cyberskills gap and ensure that there is expertise available that can protect you and your organisation.' Tony McDowell — Encryption

2.7 Other type of private platforms: Symantec Cyber Readiness Challenge

The Symantec Cyber Readiness Challenge is a cyberexercise platform designed to educate and inform IT security professionals as well as common IT users through exciting, informative and immersive user experiences in real-world, challenging events. The goal is to allow participants to test their security knowledge in a safe educational environment, and to apply their learning in their daily jobs to protect their people and information.

The challenge is a live penetration simulation, inspired by real-life security issues to help organisations understand the vulnerabilities in today's global threat landscape and ultimately gain critical security intelligence to improve their skills, knowledge and security posture. It is designed for all levels of technical expertise. It puts participants in the role of a penetration tester trying to understand the attackers' targets, technology and thought processes so they can ultimately better protect their own organisation.

This interactive 'capture-the-flag'-style competition is built along Symantec's five stages of a typical cyber breach (reconnaissance, incursion, discovery, capture and exfiltration) and leverages Symantec's leading-edge security intelligence. The exercise gives participants the opportunity to test their abilities within a unique and realistic environment and, in particular, to sharpen their security skills, expand their security awareness, implement their theoretical knowledge and compete against peers, all in a sandboxed environment.

There are a number of variations in how the exercise can be conducted, with the shortest scenario lasting no more than 2 hours, and the longest lasting for 4 to 5 full days. The level of detail of the corresponding scenarios varies accordingly, involving a variety of events and practices common to many cyberincidents and attacks. These may range from traditional penetration testing through the exploitation of lost and found devices all the way to full-scale industrial espionage operations involving intrusion and privilege escalation into IT systems, as well as the stealthy infiltration and maintenance of advanced persistent threats.

This several-hour immersion, accessible for all IT skill levels, allows each participant to develop their understanding of how security breaches can happen. The self-paced learning environment setting tasks of varying difficulty and the guided gameplay set-up supported by a hinting system create an ideal setting for participants to put their theoretical knowledge into practice in a safe environment, learn how an attacker thinks, experience how systems are compromised, and asses their security posture through a new lens. Each participant will be issued with a Continuous Professional Education (CPE) Verification of Attendance that may be used to attest the completion of training assignments or requirements. They will also receive individual performance reports based on how far and how quickly they have progressed through the chosen scenario. After its development and pilot testing phases completed in the course of 2012–13, the Symantec Cyber Readiness Challenge platform is now established so as to be able to support multiple different scenarios across the Europe–Middle East–Africa (EMEA) region. It can be accessed in multiple ways, remotely via a VPN connection or in person, or even both simultaneously. Leveraging Symantec's deep security knowledge to replicate realistic situations, the platform is designed to educate and challenge participants of all technical abilities with individual feedback. Depending on participants' requirements, the platform is able to support the co-development of further tailored scenarios.

Exercises using this platform can be run simultaneously in different locations, accommodating up to 1 000 participants, and they are underpinned by continuous remote IT support from Symantec throughout the challenge. Additional features include the option of webcasting the start of the exercise. The platform is purposely designed to be accessible even by users with only modest or average IT equipment. The minimum technical requirements for network connectivity and for participants' machines are so designed as to accommodate most commonly used hardware and software configurations without any difficulty. Even laptops that are several years old may be used, as long as the VPN software used for the exercise and the latest version of Java can be installed on them, and provided that sufficient network connectivity is available.

The platform was tested successfully in October 2013 with ENISA across different EU Member States, using a specific scenario relevant to the participating EU institutions. This fruitful experience is now available for replication ([20]) in 2014.

3. How to organise a challenge

'Hacker contest' or more?: an Austrian perspective.

Our society is filled with digital lifelines — growing with a terrifying speed and density, which we can only partly comprehend. For information technology, the limited space in the datacentre has become far too cramped and 'IT' surrounds us in our everyday life much more than we like to accept. Luckily people are also developing, slowly but surely, a certain awareness that these great opportunities also include plenty of risks for everybody. This topic has been given a lot of attention at security conferences. The 'human' factor is above all when it comes to potential risk in combination with most risk management systems, be it as user or offender. In addition, the availability of sufficient qualified personnel or 'human capital' receives plenty of attention.

The 'war for talents' — also known as the battle for high achievers — is not a real innovation. Many educational institutions orientate their portfolios to the demands of 'information and security experts'. Considering this development, the question arises of the extent to which 'hacker contests' are not just circus acts. Do the operating 'nerds' have a legal exhibition on the border of the law?

These 'outsiders', with no apparent rules and their own culture, can have a moment of public glory. Prejudices [against them] have been established due to one-sided and wrong news coverage. Are they ready to take a step into the spotlight? There are legimate reasons to think about all these questions (which are mainly due to stereotypes), but they are concealing more important facts. When officers of the federal criminal police in lower Austria managed in April 2012 to arrest the 'hacker' with the nickname 'ACK13STX', who had hacked several hundred companies in the period from January to March of that year, they were pretty impressed to discover that the criminal was only 15 years old. They were similar surprised by his reasoning. He said he was bored, wanted attention and media coverage about 'hacker' attacks — similar to those from Anonymous. These and comparable motives can be found in the statements of many other young 'hackers'.

This youthful need for admiration encounters unchallenged and irresponsible media-hyped demand. A search on Google for '16 year old hacker' yielded more than 57 000 results. This very case convinced the board of Cyber Security Austria to concentrate more on the topic of 'up-and-coming hackers'. It quickly became clear that there was a lack of consciousness of, and consequently missing opportunities and structures for, talented young people. This leads them to feel left alone with their skills, maybe stigmatised or, at best, slightly smiled at. In most cases, they just feel misunderstood by their environment. It's no wonder that many of them seek attention on different paths, and search online for people similar to themselves.

The consequences for society are crucial and far more extensive than had been expected. It is comparable to the missing awareness and structures in athletic sports that could lead to losing out

([20]) Interested organisations are invited to contact Symantec's Brussels office to discuss terms and conditions, technical requirements, scheduling options, scenario planning and logistical arrangements: Mr Ilias Chantzos Tel. , Global Critical Infrastructure Protection and Privacy Advisor, Senior Director Government Affairs, EMEA Symantec, Medialaan 38, 1800 Vilvoorde, Belgium, e-mail ilias_chantzos@symantec.com on a potential 8 seconds runner for the 100-metre sprint. That the opposite is also possible can be seen from Austria's dominance in winter sports. Professional structures were built at all levels at a very early stage, which led to a strict and hard selection process but enabled Austria to rank as one of the top nations in these sports. IT, and knowledge around its safe and secure use, is not yet acknowledged in public consciousness as a sport like skiing, but we know that we are much more reliant on IT than on the more popular winter sports. However, the comparison is perfect to illustrate the topic and intentions of the Cyber Security Challenge. The challenge is aimed at becoming the spearhead for sustainable structures that enable society to recognise young people who possess the necessary talent and interest. These 'rising stars' can then be encouraged and invested in, for as long as ordinary schooling cannot support these structures.

> *A European cybersecurity challenge should accomplish an array of functions.*

For young people with a special set of skills:

- the possibility to prove those special skills;
- the possibility to compare themselves with peers (benchmarking);
  - as a focal point and stage for young people and as a 'positive' network, where specialists from theory, science and business can communicate;
  - as an awareness and appreciation platform to get rid of stigmas — the challenge should also prove the environment of the participants how useful and important those skills are;
  - to realise their skills and how they can use these in a responsible and ethical way;
  - to adapt to their abilities and communicate them in a customised environment;
  - to get excellent perspectives from an economic, commercial and social point of view;

For business and public authorities:

- the chance to identify, encourage and develop young talents, build up a pool of talents and encourage their selective growth;
- the availability of highly qualified trainees;
- the possibility to position themselves positively for those young talents, which otherwise cannot be reached via the classic job market;
- proof of performance for local talents (benchmarking), with the results of the challenge allowing detailed comparisons;
- 'fingerprinting' to get a clear picture of the qualifications of youth in the area of computer security, more specifically the skills to intrude a computer system;
- realising available capacities;
- an event analogous to other large sporting event (Olympic Games or World Cups) to create a specific awareness and to enthuse young people about information technology;

For schools, universities of applied science, other universities and educational institutions:

- to position themselves as educational platforms for talented students;
- to proof the performance level of their own pupils or students;
- to get more young people interested in computer security — to create an awareness of the topic of security;
- to draw conclusions regarding education, science and theory.

The challenge is also beneficial for the media and society, giving them, for example, the rare chance to get a 'hacker' live in action. The challenge also shows that although 'hackers' may have a mysterious and forbidding aura, they are just ordinary people with a special set of skills. These skills are not only about misuse for criminal activities, contrary to what the majority of the population thinks.

This is why it is important not to compare all 'hackers' with offenders. 'Hackers' have a special ability to think beyond the boundaries of existing systems. Therefore, they use not referred properties and functions made by the 'designer', to utilise different purposes. With this they show that the functionality of systems always depends on the will and intention of the user. The intention that people have to adapt to the technical systems is doomed on the long run. The ones to survive on the long-term are those which are accepted and find a reasonable benefit.

To sum up we would add several general considerations.

- It makes sense to coordinate a European challenge with local partners — otherwise the overheads for running a European Cyber Security Challenge (ECSC) might become inefficient.
- ENISA should provide support in the form of clear guidelines, a European corporate identity, know-how, suggestions, White Papers and, if possible, resources (personnel and money) and a clear goal — about what is expected.
- The ECSC could be just a 'free' European comparison between different countries — but it probably makes sense to have a closer look at other successful 'working' European challenges — like the UEFA Champions League, for example. The winner of a national competition qualifies to participate in the Champions League — where the 'rules of the game' are equal and the same for all participating soccer clubs in Europe — which makes it comparable! This comparability is an important element in the basic idea of competition, on the one hand, and on the other hand it makes the challenge more attractive for the Economy to support this challenge and find highly talented young people.
- The regional approach deployed of Austria, Germany and Switzerland may provide an example.
- It make sense to coordinate the local competition between one or several public institutions, schools and universities, companies and associations. The combination of different stakeholders might also be a very important factor in organising this local challenge — because this combination provides the best coverage of potential pupils and students as well as all other supporting stakeholders. But probably it makes sense also to discuss a European prequalification which might be assisted and organised by the local players. It is not important what kind of solutions — such as 'capture the flag' or equal or open exercises like

‘hacking labs’ — are used in the local competitions or qualifications, as long as there is transparency about what systems might be used at the finals in a European challenge. But there are some advantages in running an equal system in the local (pre)qualification competitions as well.

- Because there are different school systems in different European countries, it makes more sense to divide potential participants groups by age e.g.probably 14–18, 18–30 years etc.
- ENISA should encourage the local organisers to run an additional programme — called a centre of excellence (CoE) or some other name — which supports the young talents with different services, exercises, excursions and other ‘tokens’ to enforce the network between them, as well the network between them and the economy, public institutions and the education sector.

4. Guidelines for a pan-European cyberchallenge competition

In this chapter we unfold the considerations in organising a pan-European cyberchallenge competition for students, from general information to some specifics steps foward.

The goal is to promote cyberchallenges as a focal point for:

- awareness of the need for cybersecurity and threat intelligence;
- benchmarking for young people, in schools or universities, and among lifelong learners;
- the early discovery of young people with a talent for IT security;
- understanding of the range and diversity of jobs in cyber security;
- the development of structures to sustain IT security excellence in the education sector;
- the attraction of IT and IT security for young people;
- national and European networks of excellence and establishing professional IT security excellence in Europe.

Target audience

The audience is made up of two levels, firstly policymakers who have the decision-making power and influence to lead their societies towards progress and new technologies, with citizens with high ICT skills, and, secondly, digital users, primarily students, who may get involved and develop IT expertise. Some of the advantages that we envisage are:

- the early discovery of young people with a talent for IT security;
- the fingerprinting of IT security skills of pupils and students;
- the additional promotion and training of skills (through centres of excellence);
- the professional development of young people with high potential;
- fostering of networking between themselves and peer-to-peer education;
- the provision of a clear signal to the social environment of young ‘hackers’ — we need this know-how!;
- deploy a legal environment, where skills can be developed and links made with those in cyber security jobs, to inspire and divert to socially useful jobs those who might otherwise be attracted to criminality;

- making them understand their potential and opportunities as well as their social responsibility.

Context

Furthermore, after the exchange of information from the workshop organised in April, we have noted the following points.

- There are several well-established competitions in Europe and we should take their experiences into account.
- Private organisations have developed different platforms that can be a good starting point for the pan-European platform.
- A future pan-European security challenge will be developed as follows.
  1. Based on the EU cybersecurity strategy, the first target audience will be university students and therefore the focus for the 2015 cyberchallenge will be on universities.
  2. In 2015, this publicly available report is the first document with guidelines for organising a pan-European challenge.
  3. In 2015, the language of the competition will be English , and if further funding becomes available French and German will be added.
  4. The Cyber Challenge Organising Committee is going to launch several calls, including:
     - a call for platform providers;
     - a call for general involvement;
     - a call for sponsors.
  5. The European Cyber Challenge Competition will be organised in the fourth quarter of 2015.

5. Conclusions

With this report, a milestone in this challenging initiative has been reached. We have identified the experienced players in European countries, established contact, organised the first workshop in Brussels, and published a common document as result of a highly collaborative process during 2014.

The stage is set for an ambitious deployment of the pan-European Cyber Security Challenge Competition!

Furthermore, we would like to underline the importance of the European Commission’s active involvement in getting on board policymakers in the Member States, the expertise of the EU’s cybersecurity agency, ENISA, in involving the best experts in the field and the responsibility of public and private stakeholder in understanding that the target is set very high and that they should engage to the best of their ability.

The European Cyber Security Challenge Competition is set to be the result of a public–private partnership with capable players and focused to change for the better the ICT educational approach that digital citizens in Europe receive.

References

All links were accessed during the period May–September 2014.

Legislation

EU cybersecurity strategy http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Other links

Austria Cyber Security Challenge: http://www.verbotengut.at

Cyber Security Austria: http://www.cybersecurity.at

Cyber Security Challenge UK: http://cybersecuritychallenge.org.uk

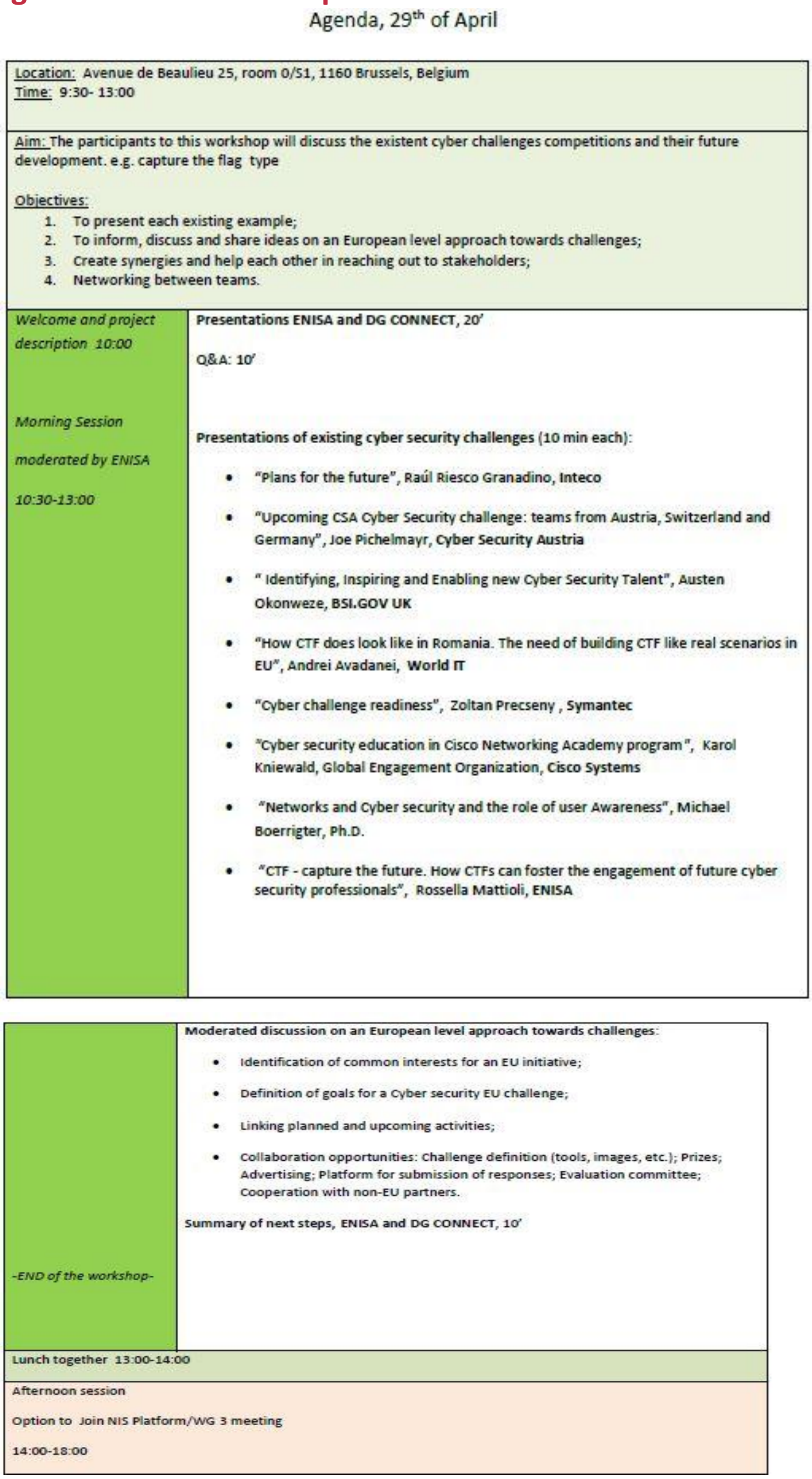
D-CTF: http://dctf.defcamp.ro

Swiss Cyber Storm: https://www.swisscyberstorm.com

Website page for this project: http://cybersecuritymonth.eu/cyber-security-challenge-competition

Spanish Cyber Camp http://cybercamp.es (live from Sept 2014)

Annex A: Agenda of the workshop



Agenda, 29th of April

Location: Avenue de Beaulieu 25, room 0/S1, 1160 Brussels, Belgium
Time: 9:30- 13:00

Aim: The participants to this workshop will discuss the existent cyber challenges competitions and their future development. e.g. capture the flag type

Objectives:

1. To present each existing example;
2. To inform, discuss and share ideas on an European level approach towards challenges;
3. Create synergies and help each other in reaching out to stakeholders;
4. Networking between teams.

Welcome and project description 10:00

Presentations ENISA and DG CONNECT, 20'

Q&A: 10'

Morning Session

moderated by ENISA

10:30-13:00

Presentations of existing cyber security challenges (10 min each):

- "Plans for the future", Raúl Riesco Granadino, Inteco
- "Upcoming CSA Cyber Security challenge: teams from Austria, Switzerland and Germany", Joe Pichelmayr, Cyber Security Austria
- " Identifying, Inspiring and Enabling new Cyber Security Talent", Austen Okonweze, BSI.GOV UK
- "How CTF does look like in Romania. The need of building CTF like real scenarios in EU", Andrei Avadanei, World IT
- "Cyber challenge readiness", Zoltan Precseny , Symantec
- "Cyber security education in Cisco Networking Academy program", Karol Kniewald, Global Engagement Organization, Cisco Systems
- "Networks and Cyber security and the role of user Awareness", Michael Boerrigter, Ph.D.
- "CTF - capture the future. How CTFs can foster the engagement of future cyber security professionals", Rossella Mattioli, ENISA

Moderated discussion on an European level approach towards challenges:

- Identification of common interests for an EU initiative;
- Definition of goals for a Cyber security EU challenge;
- Linking planned and upcoming activities;
- Collaboration opportunities: Challenge definition (tools, images, etc.); Prizes; Advertising; Platform for submission of responses; Evaluation committee; Cooperation with non-EU partners.

Summary of next steps, ENISA and DG CONNECT, 10'

-END of the workshop-

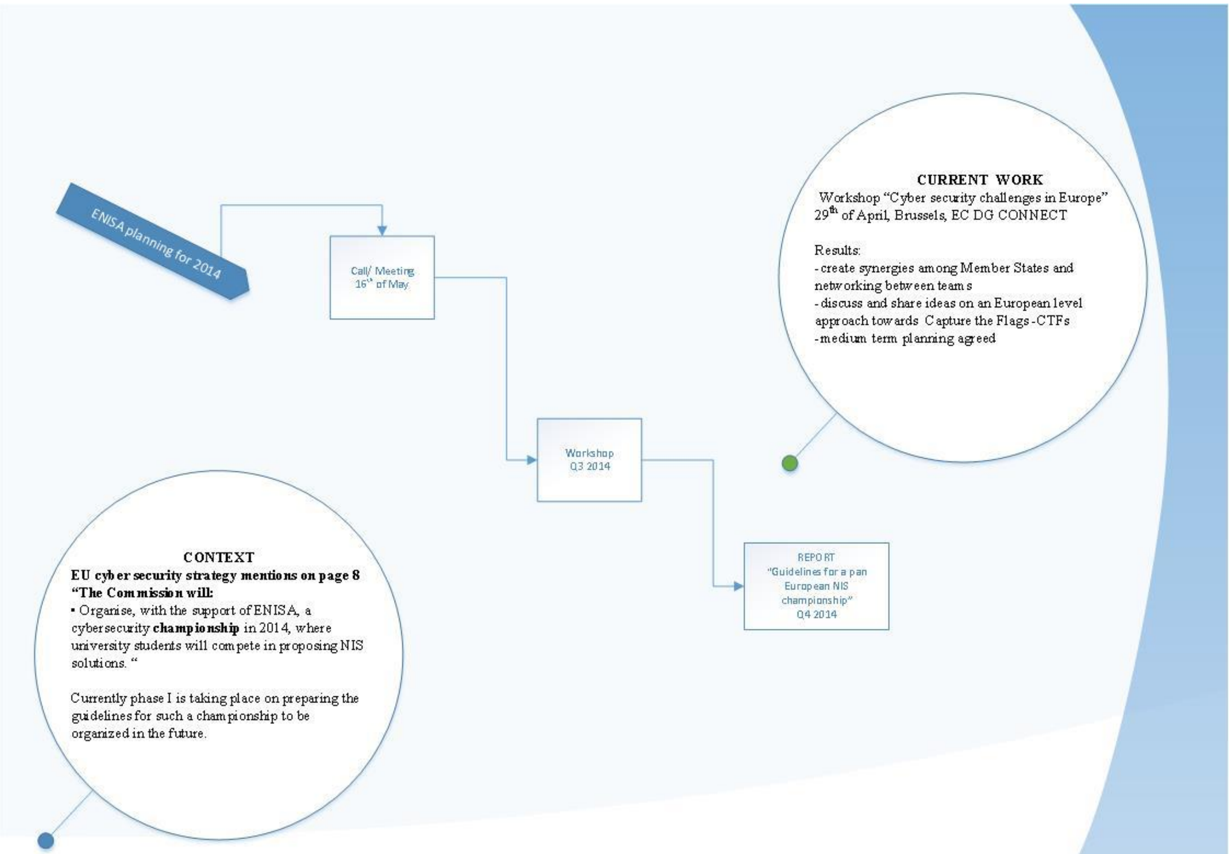
Lunch together 13:00-14:00

Afternoon session

Option to Join NIS Platform/WG 3 meeting

14:00-18:00

Annex B: ENISA planning



ENISA planning for 2014

Call/ Meeting
16th of May

Workshop
Q3 2014

REPORT
"Guidelines for a pan European NIS championship"
Q4 2014

CURRENT WORK
Workshop "Cyber security challenges in Europe"
29th of April, Brussels, EC DG CONNECT

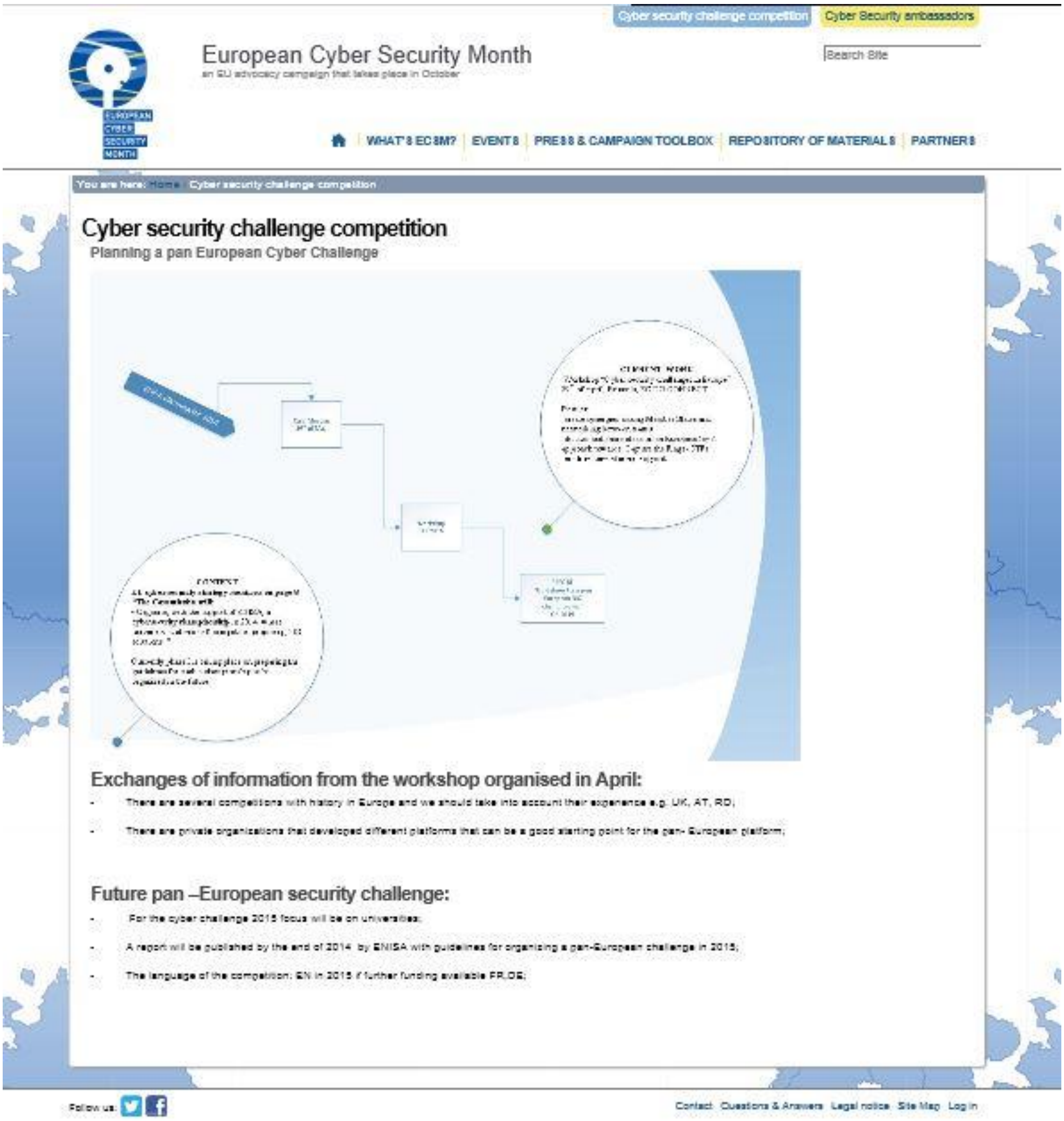
Results:
- create synergies among Member States and networking between teams
- discuss and share ideas on an European level approach towards Capture the Flags -CTFs
- medium term planning agreed

CONTEXT
EU cyber security strategy mentions on page 8
"The Commission will:
▪ Organise, with the support of ENISA, a cybersecurity **championship** in 2014, where university students will compete in proposing NIS solutions. "

Currently phase I is taking place on preparing the guidelines for such a championship to be organized in the future.

Annex C: Website page for this project

http://cybersecuritymonth.eu/cyber-security-challenge-competition



Cyber security challenge competition
Cyber Security ambassadors
Search Site
EUROPEAN CYBER SECURITY MONTH
WHAT'S ECSM?
EVENTS
PRESS & CAMPAIGN TOOLBOX
REPOSITORY OF MATERIALS
PARTNERS
You are here: Home Cyber security challenge competition
Follow us:
Contact
Questions & Answers
Legal notice
Site Map
Log in

European Cyber Security Month

an EU advocacy campaign that takes place in October

Cyber security challenge competition

Planning a pan European Cyber Challenge

Exchanges of information from the workshop organised in April:

- There are several competitions with history in Europe and we should take into account their experience e.g. UK, AT, RO;
- There are private organizations that developed different platforms that can be a good starting point for the pan- European platform;

Future pan –European security challenge:

- For the cyber challenge 2015 focus will be on universities;
- A report will be published by the end of 2014 by ENISA with guidelines for organizing a pan-European challenge in 2015;
- The language of the competition: EN in 2015 if further funding available FR,DE;

Catalogue number EN TP-04-14-678-EN-N

ISBN 978-92-9204-091-8

doi:10.2824/32650

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, GREECE

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, GREECE

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu