CYBERSECURITY COMPETENCE BUILDING TRENDS

Research report

Commissioned by the Federal Department of Foreign Affairs of Switzerland

Vladimir Radunović and David Rüfenacht

DiPLO
www.diplomacy.edu

IMPRESSUM

Cybersecurity Competence Building Trends

Published by DiploFoundation (2016)

Malta:
Anutruf, Ground Floor
Hriereb Street
Msida, MSD 1675, Malta

Switzerland:
DiploFoundation
7bis, Avenue de la Paix
CH-1202 Geneva, Switzerland

Belgrade:
DiploCentar
Gavrila P. 44a (apt 33)
Address Code 112410
11000 Belgrade, Serbia

E-mail: **diplo@diplomacy.edu**
Website: **http://www.diplomacy.edu**

Authors: Vladimir Radunović and David Rüfenacht
Editing: Mary Murphy
Illustrations: Vladimir Veljašević
Layout and design: Viktor Mijatović

Commissioned and funded by the Federal Department of Foreign Affairs of Switzerland

DiPLO
www.diplomacy.edu

Contents

Executive summary

As cyberspace becomes an essential component of our society, cybersecurity has come to the forefront of the political agenda. A growing number of reported incidents demand governments to come up with a strategic response for countering cyber-threats, especially for protecting the critical infrastructure (CI). Developing knowledgeable and competent labour for this fast-changing area is one of the main strategic challenges faced by many countries.

This research responds to an inquiry by the Federal Department of Foreign Affairs (FDFA) of Switzerland about collecting and analysing experiences from several member states of the Organisation for Economic Co-operation and Development (OECD) that have systematically advanced cyber competence building. Qualitative research was conducted from July to October 2015, based on reviews, analyses, and secondary analyses of publicly available sources. The report presents key trends and policy options for building competences in cybersecurity as identified in ten OECD countries which enjoy advanced levels of cyber-maturity: Austria (AT), Estonia (EE), Finland (FI), France (FR), Germany (DE), Israel (IL), the Netherlands (NL), the Republic of Korea (KR), the United Kingdom (UK), and the United States (US).

capacities rather than to outsource to foreign experts. Additionally, the increasing dependence of the corporate sector on the Internet has created a demand for qualified labour, which is being recognised by states as a possible driver for employment, economic growth, and global competitiveness. All the studied countries have recognised both sides of the cybersecurity coin, the risks and the opportunities, and are developing the means to transform the national labour market to meet the changing environment.

The multidisciplinary nature of cyberspace, combined with the pace of technology development, demands a comprehensive approach to building competences that goes beyond traditional education and one-off training courses for institutions and companies. All the experiences from the studied countries are heavily based on public-private partnerships (PPP), whether for support of the development and certification of new university curricula and research capabilities – and the subsequent positioning of the emerging industry in cyber-advanced regions – or for outreach to and certification of professional training programmes for public institutions and the private sector.

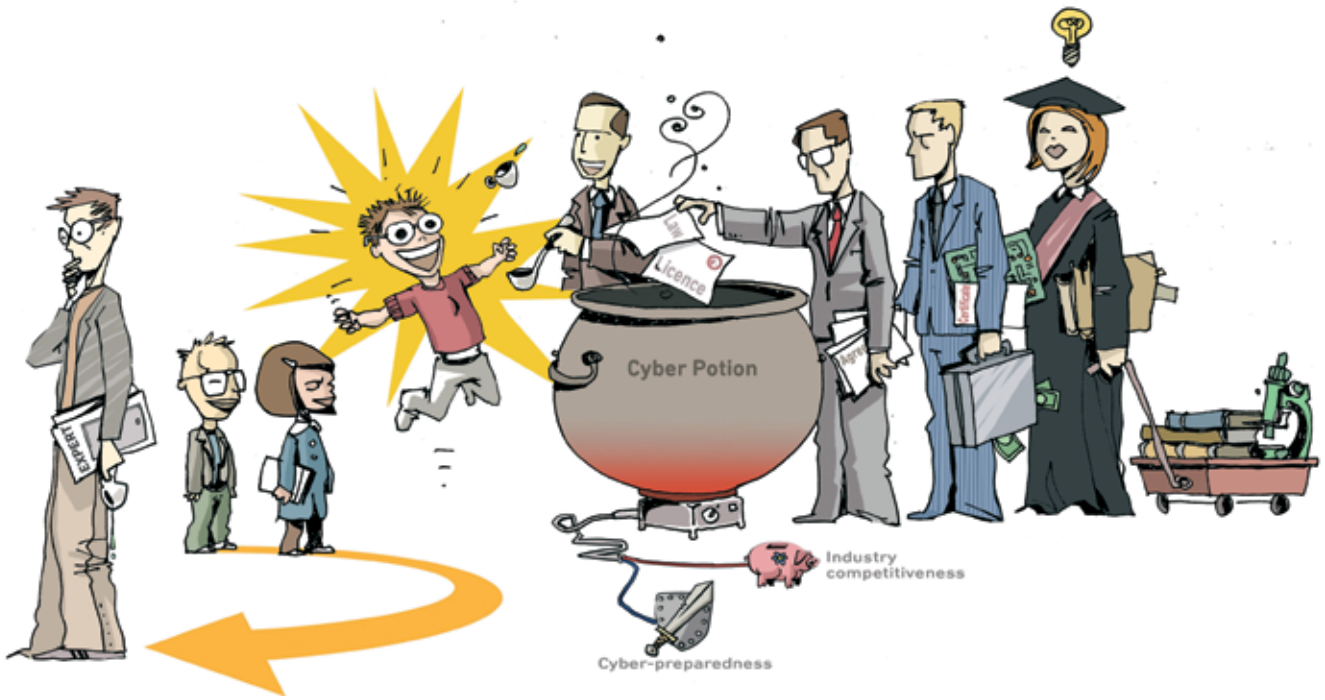

Illustration 1: Building national cybersecurity competences is powered by both risks and opportunities, and requires close cooperation by governments, the private sector, and academia.

The main driver for cyber competence building in the studied states is the demand to respond to the growing number of cyber-threats experienced, especially in critical sectors. Achieving self-sustainability and (partial) autonomy in this response, while maintaining and developing international cooperation, is an incentive for states to develop national

Looking at the experiences of the ten countries selected, several main trends were identified. All of the countries are actively supporting the development of university and research programmes. Depending on the country and its organisation, as well as its geopolitical situation, different ministries are participating in the financing of research and

training centres. A substantial element of public-private partnerships is present; with support of the governments, many of the universities and their related research labs have developed cooperation with numerous private sector partners.

Most of the larger research labs have partnered with multinational companies ranging from network technology providers such as Intel and CISCO, to general information and communication technology (ICT) companies such as Microsoft, or telecommunication providers such as Deutsche Telekom, and in some cases even defence industries such as Airbus Group SE. Such partnerships provide funds and conditions to enhance the academic portfolio, develop cutting-edge and applied solutions to technology, and increase the global competitiveness of the region and the country in cybersecurity markets. The partnerships developed at the Cyberspark Initiative in Israel, the JyvSecTec in Finland, and the Cybersecurity Centres in Germany are three leading examples that allow us to grasp their potential. Yet there are also examples of regional developments in France and the Netherlands which are being used to increase the countries' national competitiveness in the cybersecurity industry.

On the other hand, some university training facilities tend to also have partnerships with state security institutions as in cases of the UK, the USA, and the Republic of Korea. The aim seems to be to support knowledge transfer and accelerate the integration of students into the needs of their potential employers – be they the public or security sector, CI operators, or the private sector which intends to provide services to the government. The UK and the USA have taken an additional step in developing a university labelling programme which aims to encourage academic institutions to include specific knowledge in their curricula.

While these developments require larger amounts of funding and bring results on a longer-term basis, the market is also in need of short-term solutions for the current gap in qualified labour. A clear trend is the collaboration of governments with professional certification institutions which provide for a quick workforce conversion and a certain degree of knowledge standardisation.

The solutions applied by governments range from requiring certificates from private certification institutions for government or private sector employment, such as in the USA, to developing their own certification programmes in collaboration with such a private certification institution, such as in Germany. The use of private certification bodies allows a form of soft standardisation of the minimum knowledge and ability requirements for the public and the private sector, enabling rapid labour market qualification and conversion.

Several trends have identified the need for small and medium enterprises (SMEs) as well as CI operators to grasp the stakes at hand and develop their competencies in the cyber realm. The UK has recently developed its Cyber Essentials tool-kit for SMEs and requires its providers to adopt it, whereas in Germany and France initiatives were developed to support SMEs and CI operators in increasing their cybersecurity. The USA has developed a flexible Framework for Improving Critical Infrastructure Cybersecurity that companies of different size should be able to adopt.

Another trend focuses on developing targeted training programmes for managers, senior-level executives, and decision-makers. Two countries at the forefront of cybersecurity – Finland and Israel – have developed university-grade degrees and executive academic programmes in order to fill in the gap in both private and public sectors, while Germany uses an extensive professional network in order to push for manager awareness.

Finally, the lack of a definition of cybersecurity-related jobs creates a number of challenges, ranging from recruitment to training, as well as to general cybersecurity organisation within an institution. Moreover, this creates hurdles for labour mobility and lags in labour reallocation, limiting the potential for employers and candidates to find the right match. Governments, such as France and the UK, have started developing job descriptions while the USA has defined the required knowledge training for different jobs in its National Cybersecurity Workforce Framework 2.0.

All the identified policy options combine strategy led by government with the hands-on experience and the financial potential of the corporate sector as well as the knowledge and research potential of the universities. The initiatives are shaped in such a way that each of the parties involved has an interest in strengthening local expertise.

The effect of these identified trends goes beyond developing national competences for response to cyber-threats. They extend to the transformation of national labour markets and greater employment and economic growth. Moreover, in many cases this leads to the establishment of a cutting-edge cyber-industry which raises the competitiveness of states in the increasingly important global cyber-markets.

PROMOTING COMPETENCE BUILDING AT UNIVERSITIES			
University programs supported by the government	Labelling of universities	Regional development	Collaboration with professional certification bodies
Cybersecurity Centres (DE) JyvSecTec-JAMK (FI) KU Graduate School of IS and Department of Cyber Defense IS / KAIST Graduate School of IS (KR) Cybersecurity Hub within CyberSpark / *'Magshimim Leumit'* advanced cybersecurity study programme (IL) Information Technology Foundation for Education (HITSA) (EE) Austrian Institute for Technology and SBA Research (AT)	Center for Academic Excellence in Information Assurance Education (CAE) (US) Academic Centre for Excellence (ACE) (UK)	*Pôle d'Excellence Bretagne* (FR) JAMK –JyvSecTec (FI) The Hague Security Delta – Security Cluster (NL) Software Cluster Southwest Germany (DE) NATO CCDCoE / e-Citizenship & e-Government Initiatives (EE) CyberSpark Industry Initiative at Ben-Gurion University in Be'er Sheva (IL) Silicon Valley (US)	State centred model: *Expert en sécurité des systèmes d'information* (ESSI certificate by ANSSI-CFSSI) (FR) Private Sector training: US DoD Policy 8570.1 – 8410 with requirements for IA Technical and IA Management (US) CESG Certified Professional (UK)

Table: Overview of the most prominent examples

PROMOTING COMPETENCE BUILDING AT UNIVERSITIES			
State personnel training	Improving the competences of the private sector (SME and CI)	Manager and decision-making level training	Knowledge frameworks, job descriptions and professionalization
CNSS training requirements for professional training providers (US) CESG Certified Professional requirements and Certified Training scheme (UK) BSI Cybersecurity Practitioner certificate with ISACA (DE)	'Framework for Improving Critical Infrastructure Cybersecurity' by NIST (US) 'Cyber Essentials' - standards/ requirements and Certification for SME (UK) *'IT Sicherheit in der Wirtschaft'* with seminar *'IT-Sicherheit@ Mittelstand'* (DE) *'Référent en cybersécurité'* guide with standards by ANSSI and Inter-ministerial Delegation on Economic Intelligence - D2IE) (FR)	Executive Academy within CyberSpark (IL) Master's degree in Cybersecurity at JyvSecTec (FI) Korean Internet Security Agency (KISA) (KR) *Club des directeurs de sécurité des entreprises* (FR) *Deutschland Sicher im Netz* (DE) COBIT 5 by ISACA (supported by the NIST Framework for improving Critical Infrastructure Cybersecurity) (US)	'National Cybersecurity Workforce Framework 2.0' by the National Initiative for Cybersecurity Education (NICE) (US) 'Inspired Careers' (UK) *Profils métiers* job profile by ANSSI (FR)

from the studied countries (the list is not exhaustive).

1 Introduction

1.1 Objective

This report was prepared as result of an inquiry by the Federal Department of Foreign Affairs (FDFA) of Switzerland to conduct a research on cybersecurity competence building trends in order to promote competence building in Switzerland through lessons learned abroad'. The enquiry asked for collecting experiences from several OECD states that have systematically advanced cyber competence building, evaluating their experiences and outlining those that could feed into the implementation process of the national cybersecurity strategy.

The report provides a review of trends and possible policy instruments for developing cybersecurity competence based on the experiences from existing measures in ten OECD countries and based on Swiss needs in the context of implementation of the national strategy. The countries included in the study are Estonia, Israel, the Netherlands, the Republic of Korea, the United Kingdom, and the United States, as stipulated by the inquiry, as well as Austria, Finland, France, and Germany, which were selected based on a review of global cybersecurity readiness and benchmarking studies, considering also their direct relevance for Switzerland and the applicability of possible trends in the country. Particular focus was placed on policy options based on the cooperation of authorities, the private sector, and academic communities.

1.2 Background and context

Cyberspace has become an essential component of modern society. Critical societal infrastructure, the financial sector, governmental services, the security sector, schools, and hospitals are increasingly and irreversibly dependent on interconnectivity and the global network; so are the citizens. The merits of the open Internet are accompanied by threats. Some authors consider that cyberspace follows other security domains, in which security challenges are not imminent, direct, and certain any more, but rather seen as risks: 'indirect, unintended, uncertain, and situated in the future, since they only materialize when they occur in reality' (Brunner & Suter, 2008). When materialised, cyber-incidents – especially those related to the CI – may have dire consequences on functionality of state, economy, and well-being; for instance, a country-scale cyber-attack on Switzerland could result in a direct loss of more than €500 million per day (Radunović, 2013).

Such risks are distributed: any device – be it a computer, a mobile phone, or a smart light-bulb – can potentially become a weapon. Cybersecurity is only as achieved as the weakest link is secured – and the weakest link can be anywhere: from big systems to individual users. Therefore the response to cyber-risks also needs to be distributed, based on the cooperation of all stakeholders, civilian and military, government, CI, industry and SMEs, civil society, academia, the technical community, media, and end-user communities.

Prevention is based on knowledge and competence. The Swiss national strategy against cyber-risks (NCS) recognises the key role of education. For an efficient response to such distributed risks, however, there is a need to build up human skills and competences across the society, not only in certain sectors. A holistic, comprehensive, and systematic approach to education (both formal and informal), training, and capacity building is required, involving both hard competences (specific and explicit technical or specialised knowledge, individual competences), soft or social capacities including operational capacities (intercultural communication, leadership, organisational culture and values, problem-solving skills), and adaptive capacities (ability to analyse and adapt, change readiness and management, confidence), and integrated within the societal processes.

One of the most challenging issues is developing qualified labour for the cybersecurity labour market. This challenge can be seen as twofold. On the one hand there is a lack of labour in the cybersecurity labour market, meaning a lack of individuals that hold specific knowledge and capacities in order to understand the different stakes at hand. On the other, defining qualified labour is also a challenge since the tasks at hand as well as the knowledge required are still being developed.

In the last ten years, cybersecurity has developed substantially and will continue to grow as the Internet becomes ever more embedded in our daily lives. Where ten years ago, a few people could cover particular cybersecurity issues, the required knowledge today has drastically increased. This has led to new domains of specialisation that should progressively be seen as professions in themselves. Moreover, while governments may have had the biggest stake in information security and information assurance (IS/IA) in the last 20 years, the private sector is increasingly dependent on these professions due to the increased centrality of networked solutions for their business as well as their need to secure their data from unauthorised access.

[1] The Swiss Agency for Development and Cooperation defines capacity as the 'ability of people, organizations, systems of organizations, and society as a whole to define and solve problems, make informed choices, order their priorities, plan their futures, and to implement programmes and projects to sustain them' (SDC, 2006).

[2] In different technical areas, such as computer science, information security (IS), supervisory control and data acquisition (SCADA) systems, programmable logic controllers, communication and network technologies, cryptography, judicial framework, cloud computing, and geopolitics, to name but a few.

The extent of these developments has created a stark increase in demand for specialists in all cybersecurity domains while the supply of qualified labour has not increased at the same speed. Countries are now defining developing cybersecurity specialists as a national priority in their respective national cybersecurity strategies related to national defence but also to reap the possibilities of the potential economic growth the cybersecurity industry is regarded as having.

As already mentioned, another major stake is to develop standards of jobs and respective knowledge in order

- to allow employers, public and private, to identify their labour needs.
- for human resources (HR) to identify the competent individuals and their potential needs in training.
- to compile training offers that can be easily assessed and developed.

Defining standard job and task descriptions could also enable a larger cybersecurity labour market and labour mobility between government and private sector. A cross-sector standardisation of jobs could enlarge the labour market: it would allow higher education institutions to offer appealing studies with potential employment for individuals following their courses and to produce a long-term effect. The lack of common standards, such as job descriptions, tasks, and qualifications, is recognised as being a major challenge (Libicki et al., 2014).

The rapid evolution of cybersecurity-related activities has created a situation where jobs and their related tasks have yet to be defined, as well as the knowledge required to complete them. Since it is a new domain, many HR offices have difficulty assessing the quality of the applicant for jobs in cybersecurity (Libicki et al., 2014). This dilemma is further exacerbated due to unclear job and task descriptions, thus creating public and private sector recruitment difficulties.

HR departments are additionally challenged by the constant evolution of technological standards, since the emergence of new ones requires constant learning on behalf of personnel. This also demands that HR be able to follow up on trends in order to provide adequate training courses for the personnel concerned.

Finally, public and private sectors are unequally investing in networked solutions to increase efficiency and reduce costs (Gelbstein, 2015). This has created situations where IT departments may be overwhelmed, under-financed, and under-staffed in order to secure their networks. This has been compounded by the centrality of IT while often not considered or implicated at managerial level. Those companies that have developed an adequate approach tend to have invested in their IT department and the employees, as well as in their Chief Executive Officer (CEO) levels. As such, they may have the qualified labour, yet these individuals enjoy large mobility in the labour market due to their scarcity.

All these gaps demand a strategic approach and indicate the need for cooperation among various stakeholders in this endeavour. This study looks in to corresponding trends and especially the successful public-private partnerships across several countries that address these demands.

1.3 Methodology and case selection

The research question follows the problem formulation from the initial inquiry prepared by the Swiss authorities, reflecting the necessity of developing human skills and competences promoted through training and education as a requirement for developing technological and organisational measures to counter cyber-threats to CI.

The research responds to an inquiry on international trends and policy options in developing competences for cybersecurity. It is based on a Grounded Theory (Glaser & Strauss, 1967) approach. In this sense, data were collected from available sources and topics in order to gain a corpus of knowledge enabling the identification of general policies and trends undertaken in the studied countries. The research methodology includes a review of the literature (academic and policy articles, papers, and online formats), content analysis of documents (such as official web presentations and documents provided by international organisations, state institutions, corporate sectors, non-government organisations, and media outlets), and secondary analysis and official statistics (existing publicly available measurements indices, benchmarking records, and reports). The research was based on open sources, due to the fact that the cybersecurity domain is closely linked with national security, and some pertinent facts may not be publicly available.

Initiatives from various countries were looked in to, to reach an understanding of the local context, to ascertain the main ways chosen to improve cybersecurity, and to find competence-building examples. Different types of initiatives that governments have chosen were identified and clustered to be exemplified in what can be considered trends in improving cybersecurity competences. The study puts specific focus on the labelling of universities and cooperation among stakeholders, particularly public-private partnerships.

The mandate defined six initial countries of particular interest and requested a further four member countries of the Organisation for Economic Co-operation and Development (OECD) be defined during the course of the research. The initial six countries are: Estonia (EE), Israel (IL), Republic of

Korea (KR), the Netherlands (NL), the United Kingdom (UK) and the United States of America (US).

During the course of the study, three cybersecurity readiness rankings were used in order to identify top-ranking OECD countries. The Global Security Index (2014) by International Telecommunication Union (ITU) and ABI Research, the Cyber Power Index (2011) by Booze Allen Hamilton, and the report Cyber-security: the vexed questions of global rules (2012) by the Security and Defence Agenda, a think-tank that has been incorporated into Friends of Europe. A suggestion of countries be included on the research list was composed accordingly.

The main criteria for suggestion were:
- Overall ranking in the cybersecurity readiness rankings
- Proximity to the Swiss education and labour market
- Potential need for collaboration in the area of CI protection
- Publicly available information

After final consultation, the following countries were added to the selection: Austria (AT), Finland (FI), France (FR), and Germany (DE).

1.4 Focus and structure of the research

As requested by the mandate, the research has specifically focused on education-related initiatives. Nevertheless, it is important to underline that in most cases studied, education is but one of many approaches to developing qualified labour for the industry. In most cases it was the broader environment – primarily the establishment of partnerships with the private sector on knowledge incubators or certification schemes – that is understood to enable competence building. Thereby the study covered such strategic aspects rather than the available cybersecurity education programmes in the narrow sense, i.e., education at universities and professional training with a focus on cybersecurity.

The studied countries have all undertaken major initiatives and legislative developments in order to elevate their cybersecurity level. In addition, all but the Republic of Korea have undertaken new national reforms in order to meet the challenges posed by cybersecurity, not only those pertaining to CI. In order to attain this goal, the national cybersecurity strategies of most of the countries include research and education as well as awareness raising. Broadening cybersecurity education and research requires giving importance to the field of study, and emphasising the potential for employment and evolution to students and professionals. Awareness raising, job advertisements, and education promotion are thus seen as complementary push factors.

The report presents key findings about the trends and policy approaches in studied countries. The findings start in Section 2 with an outline of key drivers for government initiatives towards increasing cybersecurity competences, and some general observations on how governments have approached cybersecurity education. In Section 2, the trends are then briefly exposed before using case-study examples of policy trends that government have applied: general trends; universities supported by the government and labelling programmes; regional development university research and programmes; competence building through professional training; state personnel training; collaboration with private certification bodies; improving competences of the private sector; manager and decision-making level training; and knowledge frameworks, job descriptions, and the professionalisation of cybersecurity.

We conclude with the economic potential of the cybersecurity industry, and the means of preparing a country in order to take advantage of this.

It is important to note here that precise clustering of these emerging trends is not simple and straightforward due to many overlapping characteristics and inter-linkages. Therefore, the suggested clustering is only one possible way of presenting them.

2 Presentation of findings

To tackle the challenges discussed in Section 1, namely developing cybersecurity specialists, governments have taken a number of steps. Eight types of trends were identified during the research and are presented in more detail. Before going into the specifics of these trends, however, it is worth reflecting on several external drivers of state initiatives towards developing cybersecurity competences, and providing an overview of the identified common measures and means that governments have taken in order to push the development of cybersecurity.

The development of cybersecurity capacities at national level can be seen as a result of the eye-opening events of the late 2000s, in particular, the cyber-attack on Estonia in 2007, the Stuxnet virus attack on Iranian nuclear facilities discovered in 2010, and the ongoing espionage threats especially between the USA and China. Cybersecurity has risen to the top of the United Nations diplomatic agenda, as well as of regional organisations and multilateral forums such as the Organization for Security and Co-operation in Europe (OSCE), OECD, and the Group of Twenty major economies (G20). The importance of capacity building and the cooperation of government with industry and expert communities is emphasised in a number of political documents, which gives wind to national strategic initiatives.

The particular political driver for developing the 'in-house' competences was the Snowden revelations of 2013, which urged governments to establish additional degrees of cyber independence and autonomy. Developing competent local labour instead of hiring foreign experts for a palette of increasingly sensitive tasks improves national security, but at the same time increases local employment demand while supply is still under development.

Demands for specialist knowledge are growing as networked solutions are becoming central to daily operations in the corporate sector. This is particularly important for CI which is increasingly being operated by the private sector, but also for SMEs that lack resources to deal with the issue in spite of their high relevance for national economies. Recognising a potential for the employment of its citizens, this demand by the corporate sector for qualified labour is recognised by states; in turn, states are developing the means of adapting national labour to the changing labour market. This labour market transformation is seen by countries as the key element for the twenty-first century competitiveness. For example the USA has recently launched a national programme, the Tech Hire initiative, for workforce conversion. Its aim can be broadly seen as twofold: to reduce unemployment by training individuals where there is a strong labour demand, and to develop US competitiveness. This is also the case in countries such as France, Finland, Germany, and Israel as well as the United Kingdom, where national cybersecurity initiatives also aim at positioning the countries as leaders in the export of cybersecurity products, services, standards, insurance, research, or education.

The policies adopted in these cases, therefore, target two objectives: developing cybersecurity capacities in the country and supporting economic growth by positioning the country in the developing cybersecurity market. As a consequence of these measures, the education market in the cybersecurity domain increases, creating a potential for attracting partnerships with companies.

One of the main characteristics of cybersecurity education and research development in the studied countries is the extensive use of PPP. Some of the main reasons for this identified in the study are as follows:

- Many institutions, private and public, do not have the know-how to develop their capacities and thus turn to professional training and certification bodies (in cybersecurity, but also IT governance and information security management systems). Due to the recent emergence and rapid expansion and evolution of cybersecurity professions, there are limited professional and internationally accepted standards, and companies such as CompTIA, CISCO, CREST, EC-Council, ISACA, ISC2, and SANS that provide training and certification, can be seen as driving the standardisation of knowledge through the reputation of their certification. In many cases, private sector companies are already demanding that their cybersecurity specialists hold a specific certificate from one of these providers; hence PPP is for mutual benefit.
- Most developed economies depend heavily on IT infrastructure and require the means to mitigate cybersecurity risk, including industrial espionage. States have direct interests in protecting their corporate sector, especially the CI which is increasingly operated by the private sector.
- In order to develop a long-term supply of qualified labour, states are interested in developing pools of knowledge and research within academic institutions. This is enabled by the environment that attracts investments by the companies in joint ventures, research hubs and start-up incubators in partnership with universities and national and local authorities.
- At the same time, such partnership with authorities and universities benefits the ICT industry in strengthening their cybersecurity product development and export, which in turn enables the state's competitiveness in a global cybersecurity market.

In most cases, these common approaches to increasing the cybersecurity labour market were accompanied by the introduction of regulations and requirements for the state and its suppliers. The research shows that at least eight countries (AT, UK, FI, US, DE, FR, EE, NL) have adopted new and stricter regulations pertaining to IS and/or particularly CI operators. This is seen as a general step in creating the necessity for IS and for CI operators to further develop their security infrastructure. These norms generally require state agencies, CI operators, and government providers to adhere to minimum security standards. In some cases, specifically for CI operators, the framework may require announcing any breach of security to

the national regulatory authority. Such a general framework requires companies to ensure a safe computer/network environment as well as minimum protection for sensitive data, which may stimulate the labour market demand for cybersecurity specialists capable of ensuring the required regulations responsibly. This seems to create a potential career path for individuals seeking education and employment, and consequently boosts the training and education market. Finally, a clear and transparent legal framework for IS, defining the roles, responsibilities, and accountability can create an attractive environment for researchers, companies, and customers worldwide.

Looking into the experiences of the ten selected countries, several main trends were identified. On a long-term scale, governments tend to support the development of new university programmes both financially and through creating the environment for investment by the private sector which can lead to the development of regional hubs, but also through certification and labelling of particular study programmes of interest and in line with national demands. Looking for a short-term response to demands for quality labour, governments turn to professional training and certification of private and public sector personnel – technicians, managers, and senior-level officials – through programmes shaped and provided in cooperation with the corporate sector, especially the private certification and training institutions. This process is also supported through attempts to professionalise the cybersecurity market by developing job descriptions and knowledge frameworks.

2.1 Promoting cybersecurity competence building at universities

Strengthening the university curricula is the most important long-term step towards sustainable national competences identified by many governments. Strategic recognition by governments of a need for qualified cybersecurity labour and the demand from the private sector is what drives universities to introduce new thematic coverage and majors.

The two clearly identified policy instruments to promote competence building at universities are government support for developing training and research programmes – both in terms of finances and an environment to facilitate cooperation with the corporate sector – and certification and labelling of the universities and study programmes.

Another specific trend was identified which promotes private sector investment in education, research, and development activities in universities in particular regions. Such investments lead to establishing innovation hubs and start-up clusters around the universities selected, which creates a fruitful environment for multidisciplinary and cutting-edge research and education while at the same time boosts the industry competitiveness of a region and of the country.

2.1.1 University programmes supported by the government

There are several examples of government partnerships with universities for initiating cybersecurity-type curricula. Since 2011, the German Ministry of Education and Research (BMBF) has been sponsoring research in cybersecurity as well as supporting a group of educational institutions in this realm: the German Cybersecurity Centres. In the framework of these institutions, the BMBF, in collaboration with the Ministry of the Interior (BMI), has been supporting cybersecurity certification. The centres boast private sector appreciation and are part of the larger Frauenhofer Institute network which aims to boost research and collaboration between academia and the private sector.

In Finland, the JyvSecTec (Jyväskylä Security Technology), a cybersecurity research, training, and development centre founded in 2011 and attached to the JAMK University of Applied Sciences, is financed by numerous Finnish Institutions. It has been promoted by Tekes (the Finnish Funding Agency for Innovation) Strategic Centres for Science, Technology, and Innovation in Internet economy (SHOK) and also as part of the Innovative Cities programme established by the Ministry of Employment and the Economy. For the last two years it has been used as the main facility for the Finnish Defence Force's delegation for the NATO Locked Shields exercise. In addition to its education and training services, it offers research and consulting services. It currently offers a professional Master's degree in Cybersecurity that will be further discussed later in the paper in the manager and decision-making level training section.

In Korea, there are several examples of partnerships between government and universities. The Korea University Graduate School of Information Security was established in 2000 in partnership with ministries and the police as well as private partners such as Samsung and the US Department of Defense (DoD). The curriculum focuses mainly on technical aspects including cryptography, networks, and new technologies, with some elements of industry, cyber law, and incident response. Several majors have been introduced in recent years, such as privacy, financial security, cybersecurity majors, and public security policy. The Korea Advanced Institute of Science and Technology (KAIST) Graduate School of Information Security was established in 2010 with support of the government, providing Master- and PhD-level degrees as well and covering a wider palette of aspects including policy, law, and economy. Korea University has established the Department of Cyber Defense Information Security in partnership with the Army Cyber Command, which offers scholarships for the four-year programme. The department trains 1% of elite cybersecurity professional officers to be ready to combat cyber terrorism and the threat of cyberwar. Students are recruited mainly by the Armed Forces but also by companies and public institutions.

In Israel, the Ben Gurion University has become a research and educational cybersecurity hub within the strategic Cyber-

Illustration 2: *Long-term effects on cybersecurity are enabled by strengthening university curricula and research capacities through financial support by the public and private sectors.*

Spark Industry initiative which will be discussed in greater detail later in the paper. The Israel National Cyber Bureau (INCB) has initiated a Magshimim Leumit advanced cybersecurity study programme in leading high schools, mainly targeting outstanding students aged 16 to 18. This comes in response to Israel's specific security context. The curriculum focuses on programming languages and building algorithmic thought processes, understanding the structure of computers and the Internet, and analysing computer systems and developing creativity which may also be used for future start-ups.

Estonia has created the Information Technology Foundation for Education (HITSA – Hariduse Infotehnoloogia Sihtasutus). It is a PPP with the Ministry of Education and Research and universities on one hand, and Estonian ICT companies on the other. The programme aims to develop ICT competences on all levels of education. It also aims to teach ICT in graduate programmes not only in cybersecurity and ICT, but also with an emphasis on domains ranging from health to smart housing and materials where ICT can add value.

Austria has also taken steps to promote and develop its cybersecurity and research domains. In addition to its online platform gathering information ranging from security warnings, tips for online safety for consumers, and research and education programmes, it has established a number of research programmes supported by the Austrian Research Promotion Agency (FFG), and two research institutes: the Austrian Institute for Technologies (AIT) and SBA Research. While AIT is more focused on bridging the gap between academia and industry and includes a number of ICT projects, SBA Research focuses only on IS. SBA Research is a Competence Centre for Excellent Technologies (COMET) funded by the FFG, which develops research and training for the public and private sectors. It has become the largest Austrian non-university research lab in IS. Its partners include universities and research centres but also a large range of private sector companies.

Many of these programmes support research labs or incubators because they allow the development of strong PPP and applied research. As ICT and cybersecurity technologies need to be easy to use, ready to be incremented, and require real-world testing, this also raises the interest of private sector partners. Finally, many of the countries that are supporting universities and research labs also support them in creating global outreach programmes.

2.1.2 Labelling of universities

In the long run, developing cybersecurity university programmes should provide an adequate amount of qualified labour. Besides subsidising and creating incentives and collaborations with universities and research labs, two countries have decided to certify and label universities and study programmes: the USA and the UK.

The idea of certification seems to originate from the US National Security Agency (NSA), which established its first university outreach programme, Center for Academic Excellence in Information Assurance Education (CAE-IAE), in 1998.

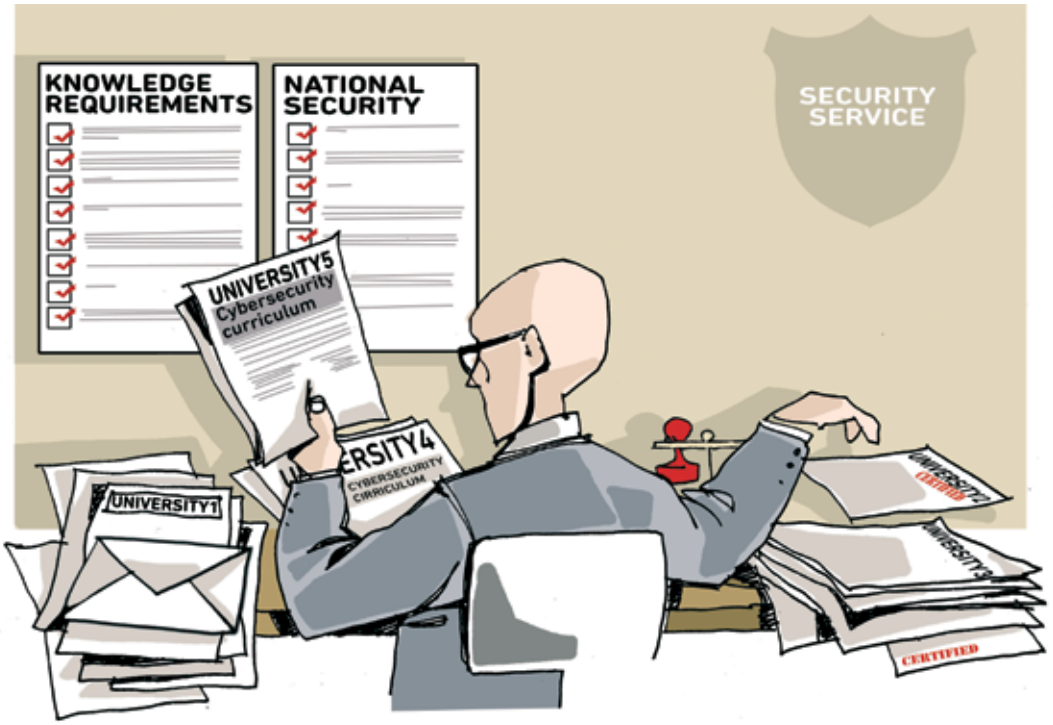

Illustration 3: Harmonising certain university curricula with national security knowledge requirements may attract students and train future government employees, but also brings risks of politisation.

It received a further push when the Department of Homeland Security (DHS) joined in 2004 and it has subsequently been renamed the Center for Academic Excellence in Cyber Defense. All universities are eligible for CAE certification. There are four categories of CAE certificates: technical institutions, universities, research qualified institutions, and specialised research institutions. In order to be accredited, universities must fulfil certain criteria, such as establishing a cybersecurity institution on their premises and teaching in-depth courses on a certain number of cybersecurity Knowledge Units (KUs) which are closely related to the Knowledge, Skills and Abilities (KSAs) presented in the Cybersecurity Workforce Framework 2.0. This will be discussed more in detail further on. Once the National IA Education & Training Programs (NIETP), a programme run by the Information Assurance Directorate of the NSA, issues a certificate for a particular university or institution, it is valid for five years. There are currently over 183 CAEs in different domains recognised by the NIETP.

In 2008, the NSA and the Committee on National Security Systems (CNSS) briefed the Five Eyes members (Australia, Canada, New Zealand, the UK, and the USA) of their programme. The UK Academic Centre for Excellence (ACE) initiative can be seen as an English variation of the programme.

The UK programme is establishing itself in a similar way with an interim step of certifying Master's degrees before certifying universities themselves. Since 2012, the UK Government Communications Headquarters (GCHQ) and its partners have certified 13 universities as ACE in Cybersecurity Research where the main focus is on research. The model seems very close to the US version, albeit the GCHQ has published a statement encouraging academic research independence and does not seem to have the same depth of knowledge description, at least not publicly available.

The second step of the UK initiative is to develop education-oriented ACEs. It is doing so by first testing individual Master's degrees with the aim of certifying the university or one of its faculties as ACE in Cybersecurity Education. The idea is to start with Master's degree certification and then have universities become certified as ACEs in Cybersecurity Education (starting 2016). Thus, since 2014, the GCHQ has been inviting all universities to submit their Master's programmes related to cybersecurity for GCHQ certification. This process contains two phases: the Provisional Certification for degrees where students have not yet completed a degree and Full Certification for courses that have been completed by students. Until now, 6 universities have been granted a total of 12 certified Master's degrees.

The idea behind the initiatives is to stimulate development of higher education and research offers in the domain while establishing national education requirements (such as KUs in the USA) that the universities requesting certification must meet. An advantage of this system for the authorities is their direct involvement with the university research and education system, allowing closer ties with academic research (following research but also developing research in their required areas). Besides, it gives them two advantages related to new labour. First, the students graduating from these universities will have followed a syllabus partially developed by the NSA/GCHQ allowing them to be more quickly

integrated into their future jobs. Secondly, the presence of the NSA/DHS liaison officers, called a Security Education Academic Liaison (SEAL) representative in the US model, enables the government to scout for 'outstanding students for future government employment'.

In the US and UK versions, certification in these cases helps universities become more prominent through the use of a label issued by an internationally recognised intelligence agency: many universities in the USA (it is too early to evaluate the UK model) were able to attract potential students by using the NSA labelling. The second incentive is the existence of a SEAL representative appointed by the NSA. For universities, the representative can be interesting since their role is to promote the current state of research in cybersecurity and define the mutual interest between the government and the institution. This may boost the possibility of better formulating their objectives for accessing research funds and additionally qualifying for specific funding from the DoD. In the USA, the financial side also seems very important for the students, since in most cases they will be able to enjoy a full scholarship – the Cybercorps Scholarship – which partially explains the higher enrolment. Yet since the Snowden revelations, some universities have faced stark criticism by faculty staff and students due to the links with the security agency. Effectively, the programme has witnessed its first students opting out of the scholarship.

2.1.3 Reaping the economic potentials: regional development

A particular trend was identified in a number of countries which boost competences as result of a response to economic potentials of cybersecurity rather than to risks. In order to attain a leading position in the new domain, several countries (EE, DE, IL, FR, FI, NL) have decided to boost their cybersecurity industry by investing in education, research, and development activities in specific regions, establishing innovation hubs and start-up clusters. In all cases, the key component is a cooperation of government, academia, and the private sector.

Most countries are not developing regions from scratch but using pre-existing educational and scientific potential and structures, and supporting their development in the sphere of cybersecurity. France has push for a centre of excellence (pôle d'excellence) in Brittany where some of its most reputed engineering schools are located, as well as its centre for military instruction. Finland has supported the development of the JyvSecTec in Jyväskylä where high-tech industry had already been developing. Germany and the Netherland have been developing their education under the term 'cluster development'. Germany has its software cluster around the Rhineland-Palatinate state (it extends in the neighbouring regions and is relatively near Bonn where the Federal Office for Information Security (BSI) is headquartered). The Netherlands has its Security Delta in The Hague, where the main administration is. To develop their regions and industries, Finland and Germany, and also Estonia, have made use of regional subsidies offered by the European Union.

Estonia, due to its size and the 2007 cyber-attacks, can be seen as a region in itself, developing its cyber capabilities and notably cyber education through development policies. It is the location of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) and has also gained access to the European Union development funds which it has allocated to IT and cybersecurity education. In combination

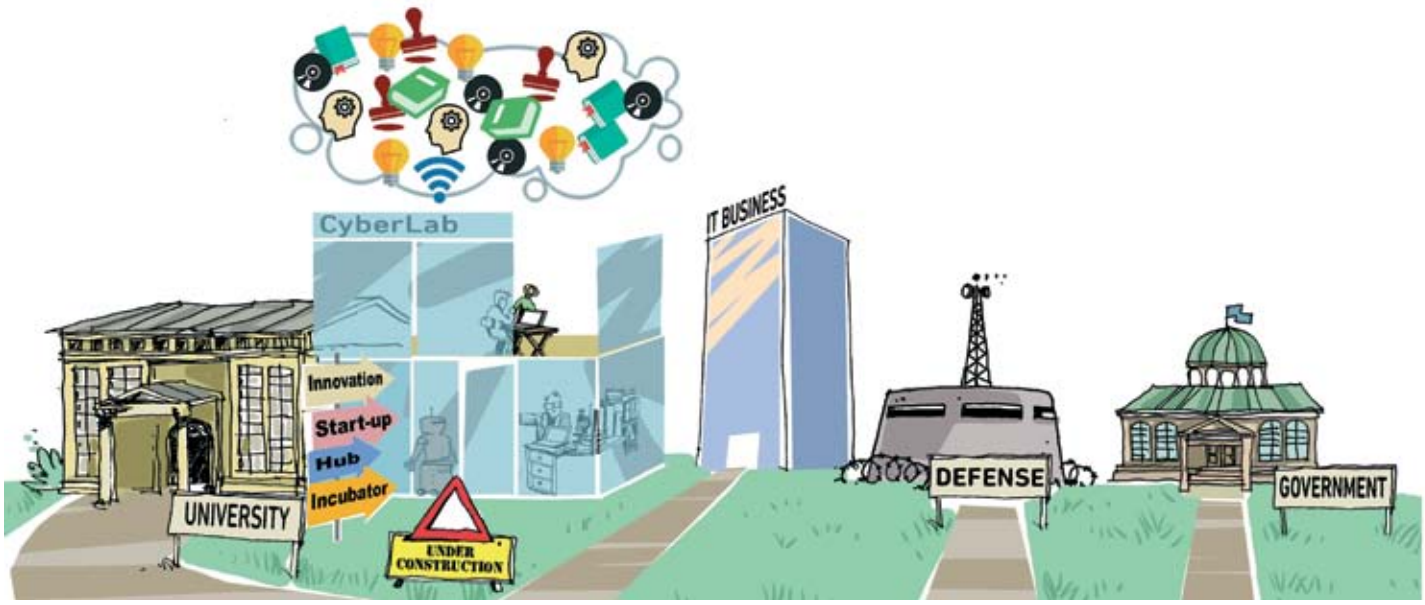

Illustration 4: Developing a cybersecurity industry through innovation hubs and joint ventures attached to established universities strengthens national competences and competitiveness on the global market.

with its e-citizenship and e-government initiatives, it enjoys a very good reputation in cybersecurity.

The least specific is the US case where the most well-known ICT region is Silicon Valley which stands out. Yet the size and organisation of the country allows for more centres with a current development on the East Coast.

The most impressive development with regard to budget and speed is the Israeli development of the city of Be'er Sheva (near its main intelligence-gathering installation) with its CyberSpark Industry initiative, aiming to position it as a global cyber centre. The CyberSpark Industry Initiative is a multi-year strategic endeavour of the Israeli government, formed as a non-profit organisation as the coordinating institution for joint cyber-industry activities with government agencies, the defence forces, academia, and global and regional leaders of the IT industry. The Ben-Gurion University benefits from high-level investments in its resources and research and development (R&D) capacities as well as from promotion and positioning. The corporate partners benefit from having access to the most advanced cyber labs and talent in the proximity of the major universities and defence and intelligence units; establishing R&D centres (such as the Cyber Security Research Center) and centres of excellence and education centres (such as the CyberSpark Executive Academy previously discussed in the section on manager and decision-making level training), starting joint ventures, tech incubators and innovation centres; and initiating joint research with university labs. The Cyberspark Industry initiative is a direct response to the Israeli aim to become a global cyber superpower, and the world leader in cybersecurity, as expressed in its National Cyber Initiative policy. At the moment, Israel is the second biggest worldwide exporter of cybersecurity products and services, behind the USA.

In all cases, the aim of these regional developments is to use cybersecurity education and research not only in the interests of national security, but also with the aim of reaping the potential rewards from the economic and labour boom that the cybersecurity and the more general IT sector are seen to have. Moreover, the initiatives were not developed from scratch but were located in areas that already had an existing infrastructure or labour pool. Depending on the nature of the state or its membership of the EU, governments are appealing for different kinds of support funding, but all fundamentally rely on private investment and PPP.

These several examples are just few of many that seem to be growing – with or without direct government support – in most of the countries explored. The approach for creating such regional centres, for hosting centres of excellence, and for building R&D capacities and business incubators appears to be the increasingly relevant and following a trend, since it can enable cooperation and cutting-edge knowledge with major investments coming from the private sector.

2.2 Competence building through professional training

Developing university programmes can be seen as a long-term solution for increasing the supply of labour and achieving an edge in research. Yet governments and the private sector already need this type of labour, and in many cases professional training has currently taken the lead. In order to develop the competences governments and private sector employees need, a number of trends have been identified.

While state personnel training has been implemented through different means, a challenge that is often met is that of labour mobility, i.e., a government employee or a private sector employee could move between the two markets without facing long periods of training. An important element here is the lack of common standards.

Government collaboration with private certification bodies, using the knowledge and training offers at hand, can create a temporary common standard in order to attain such mobility. It also provides a short-term solution until specific university programs are developed, while also allowing for quick 'hands-on' training for individuals with basic knowledge.

While government and large corporations are adopting policies to secure their networks and infrastructures, SMEs tend to still lag behind while they are the largest employers and potential supply chain elements for governments. A number of policies aim at developing awareness in cybersecurity and raising the minimum security of these important elements.

The general demand for cyber-specialists is growing in both sectors. Yet, there is still a lack of awareness at the mid- to top-level management level with regard to IT security which tends to hinder investment in suitable, secure solutions. A small number of educational institutions have developed courses especially targeted at mid- and top-level executives in order to complete the picture.

Finally, as already mentioned, one of the main challenges facing recruiters in all cybersecurity domains is the lack of common definitions of jobs as well as minimum standards of knowledge. A major development in this area can be seen as the professionalisation of cyber tasks into fully fledged jobs with related knowledge, skills, and abilities. If these were to exist this would also allow professional associations that define the requirements, a task that some states have started to support by developing knowledge frameworks.

2.2.1 State personnel training

Prominent models for state personnel training exist in the USA, France, and the UK. In these cases, general state personnel training in Information Assurance (IA) has existed for a longer period of time. In all three models, state employees are required to hold a minimum security clearance requiring

a background check (such as the Baseline Personnel Security Standard in the UK). Where these national initiatives differentiate the most is in the teaching-learning process.

Whereas UK and US training programmes tend to rely on private actors, France has a more state-centred approach with the accreditation body being the French Network and Information Security Agency (ANSSI). ANSSI is the only authority entitled to deliver the certificate for information security to state personnel – the ESSI certificate (expert en sécurité des systèmes d'information). The target public is state employees who, during the course, will acquire knowledge ranging from legal aspects to cryptology and information security. It can be obtained at ANSSI directly through its Information Systems Security Training Centre (Centre de formation à la sécurité des systèmes d'information – CFSSI), which was founded by a 1986 decree. Once the educational and security criteria have been met, a state employee can follow a full-time 13-month teaching period. Another possibility is to have ANSSI certify an employee's experience and knowledge through its validation process (validation des acquis de l'expérience). ANSSI trains around 1500 government employees per year in Information Security.

In the USA, the DoD Policy 8570.1 Information Assurance Training, Certification, and Workforce Management (now being replaced by the DoD 8410 Directive) sets the requirements for state personnel, which are often referenced with certification programmes issued by private sector professional certification bodies (such as CompTIA, CISCO, ISACA, ISC2, Mile2, and SANS). The certification model for state personnel is broken down into two sectors of knowledge – technical and managerial. For technicians, Information Assurance Technical (IAT) certificates are broken down into three levels going from computer literacy, to network environment, and finally global environment. The DoD maintains a list of private sector certifications that teach the required technical knowledge in order to pass each level. At managerial level, the Information Assurance Management (IAM) is also broken down into three levels: IAM I, IAM II, and IAM III, with same thematic coverage as the IAT, but focusing on managerial and supervisory responsibility. The DoD also maintains a list of private certificates (given by CompTIA, ISACA, ISC2, and SANS), that attest a minimum standard of knowledge for each level. These certifications can be attained through regular classes, self-learning, or boot camps, which are generally 5-day periods of intensive training followed by a certification exam. The certification is either paid for by the employer or the employee, depending on individual circumstances.

In the three cases (UK, US and FR), regulatory frameworks may require that a contractor or a government supplier provide the certification for their own employees aiming at securing the whole supply line and thus pushing up the general cybersecurity in the private sector as well. In the UK, this is covered by the Cyber Essentials certification that will be discussed later on.

The advantage of the US certification system is that it enjoys the recognition of both the state and the private sector, since it is based on the work of professional certification bodies. The US policy may hold another advantage since any individual may obtain private sector certificates, which then have equivalences in the federal system thus allowing for easier labour commutation between the sectors and simplifying recruitment on both sides, consequently creating a common cybersecurity labour market. This is also the case in the UK with the development of the CESG Certified Professional (CCP) platform where professional certification bodies can validate their products as explained in the following section that reflects on collaboration between governments and private sector certification authorities.

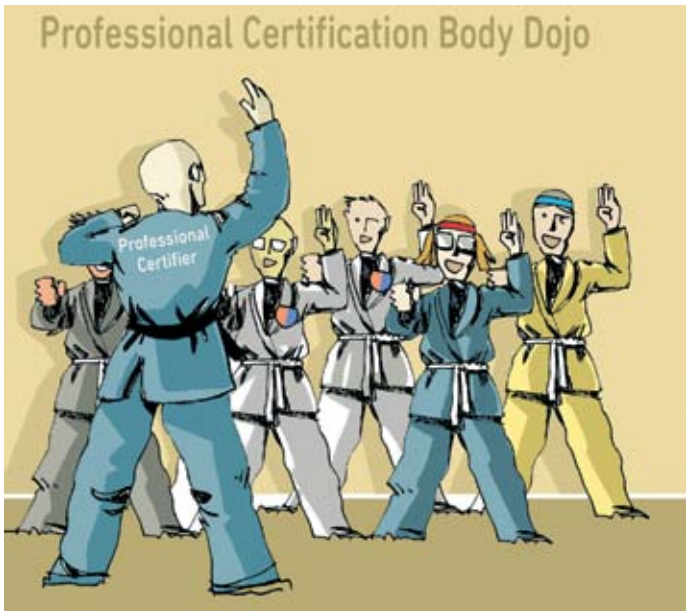

***Illustration 5**: Using professional certification bodies for state personnel training reduces the costs and encourages workforce mobility, while in-house training brings greater control and specialised focus.*

2.2.2 Collaboration with professional certification bodies

Some governments have decided to define their state personnel training based on existing private certification offers because the industry has pioneered and mastered cybersecurity training and certification way before the government. Besides utilising this for the benefit of the public sector as previously discussed, some governments have partnered with professional certification bodies to also strengthen competences in the private sector and make them compatible with those in the public sector. This strengthens the common cybersecurity labour market and also enables the secured cooperation chain between the public and private sector in different fields.

In some of the studied countries (e.g. DE, UK, US), private-sector-based professional certification bodies that hold highly specialised knowledge in cybersecurity have been accompanying the general process of developing qualified labour. One of the advantages of recognising and working with these bodies is that their hands-on knowledge transfer allows for rapid labour qualification. This is very strong in the USA where most of the major private cybersecurity certificate providers are based. Recognising this potential, the US government has developed regulatory norms in close collaboration with some of these partners over the last 10-15 years, while allowing said partners to integrate these regulatory norms within their different syllabuses. Furthermore, the US government Committee on National Security Systems (CNSS), which establishes standards for the government IS system, has issued certificates for professional cybersecurity training providers over the past few years. The CNSS label attests that the courses given by the private sector meet the official CNSS training requirements (4011 to 4016 IT security training standards),

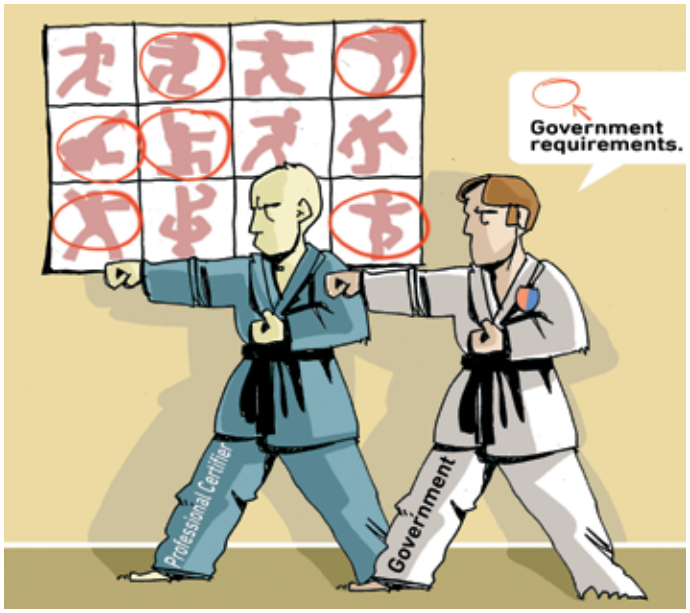

Illustration 6: *Cooperation between government and professional certification bodies on creating certificates adjusted to national environment also strengthens the national policy framework.*

thereby adding value to professional certificates that comply. A benefit of this cooperation with the professional certification bodies is a quick and relatively cheap training (compared to regular US university fees) for labour adapted also to government regulations and requirements.

More recently, the German Federal Office for Information Security (BSI) has developed a Cybersecurity Practitioner certificate with the German chapter of the professional certification body, ISACA, though there is no detailed information available publicly. It seems that the certificate was developed within the Alliance for Cybersecurity framework; no further information on this was found. In this case, the use of a private company most probably allowed the BSI to develop a rapid labour qualification while creating a win-win situation with the provider, ISACA. The Alliance for Cybersecurity (Allianz für Cyber-Sicherheit – ACS) was founded in 2012 by the BSI, in collaboration with the Digital Association of Germany, BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.), and aims at promoting and increasing Germany's resistance to cyber-attacks. The entity also provides an overview of upcoming trainings, seminars, and conferences as well as tools German companies can use to develop their cybersecurity capacity.

Finally, the UK National Technical Authority for Information Assurance (commonly referred to as the CESG – Communications-Electronics Security Group, closely linked to the GCHQ) has developed the CESG Certified Professional in close collaboration with the private sector and APMG, an international company that accredits training and manages certification schemes, as the entitled certification reviewer. This CESG-issued certificate, alongside with its Certified Training scheme, requires private sector certificate suppliers to submit their course syllabus to APMG which will then certify that it meets the CESG requirements. Approval will allow the provider to use the CESG logo and advertise its training as officially validated just as with the USA's CNSS.

In general, the promotion and certification of private sector education firms allows quick labour force education and reconversion while potentially keeping the costs outside of the state budget. Moreover, many of the new regulations for government institutions issued in recent years require government suppliers to comply with the same IS regulations; validating professional certification providers to train the private sector that acts as a government supplier alleviates the need for regulatory authorities to devote a large number of training hours to validate the cybersecurity capacities of third parties. In the certificate providers' view, this collaboration is also a win-win situation: by collaborating with the government in developing the regulation and aligning their curricula with regulations, their certificates gain formal recognition and relevance. Given the number of certificate providers and the competition among them, each one has an interest in having its certificate recognised as being closest to the regulation requirements and accepted by the largest number of regulatory authorities while remaining vendor- or state-neutral.

In a recent study by the RAND Corporation, Hackers Wanted (Libicki et al., 2014), the researchers noted these advantages among others. An additional remark was that in some cases the certificates also allow HR personnel to recognise the potential knowledge of the applicant, since in many cases they are also new to the cybersecurity domain and do not know what to expect from an applicant. On the downside, some of the HR personnel as well as cybersecurity professionals interviewed noted that certificates do not give satisfactory evidence of the candidate's ability: due to the quickly changing environment, individuals who learn quickly and who persevere may be better suited to the job in the long run than individuals holding certificates only.

In summary, the use of certificate providers enables rapid labour market qualification and conversion, helps assess the candidate's profile, and may train more people in less time in the case of new state regulation introduction.

2.2.3 Improving the competences of the private sector

The importance of the security of corporate sector is recognised in most of the countries studied. While there are almost no specific programmes identified for CI operators, most of the measures directly apply to them since in most OECD countries CI are operated by private companies.

In the USA, however, the National Institute of Standards and Technology (NIST) has developed a framework called the Framework for Improving Critical Infrastructure Cybersecurity. In collaboration with the private and government sectors, this voluntary framework was developed in order to create a common language with regard to cybersecurity management, facilitating the workforce flow between the private and the public sector as well as defining agreed upon procedures. The framework also provides guidelines for federal agencies for complying with current regulation. It gives a flexible step-by-step approach to handling cybersecurity for organisations of different sizes. It also incorporates and references different certifications provided by private entities as well as national and international norms enabling specific training and norm compliance.

Several countries are particularly emphasising developing measures for SMEs – ranging from best practices guides, to teaching and training offered by state institutions – for the following reasons:

- In many countries, SMEs represent the largest number of businesses.
- In comparison to bigger actors, SMEs often don't have the resources to adequately train their employees, update their infrastructure, or have their own incident response team.
- In many cases, SMEs are also providers in governmental supply chains, including CI, thus there is a need to strengthen their competences in order to minimise the potential security breaches into government infrastructures.

Realising that SMEs are in this particular situation, the UK government has vowed to support their needs for ensuring cybersecurity. This led the British Standards Institute, in collaboration with private entities, to develop its Cyber Essentials, published in 2014, a set of standards and requirements an SME can put in place. Moreover, it has set out the requirement that all government suppliers must apply for the Cyber Essentials Certification in order to acquire a government contract. Finally, the UK government has set out a budget to offer SMEs a £5000 voucher for cybersecurity advice.

Illustration 7: *SMEs and CI operators are often weak links in the cybersecurity chain; governments can assist them by establishing standards and certifications, issuing guidelines, and offering training.*

Germany has set out on a similar plan for raising awareness and training with SMEs. The Federal Ministry for Economic Affairs and Energy (BMWi – Bundesministerium für Wirtschaft und Energie) has developed the IT Security in the Economy initiative (IT Sicherheit in der Wirtschaft) which aims at raising awareness of IT security. The activities are less focused on purely technical approaches, but aim to create a general understanding of the importance of IT security. One of the educative activities is the IT-Sicherheit @ Mittelstand – a half-day seminar provided by the Association of German Chambers of Commerce and Industry. The target audience is managers of SMEs and the class aims to create not only awareness but provide reasons and incentives for better managing IT security.

In France, the Inter-ministerial Delegation on Economic Intelligence (D2IE) with the support of ANSSI published a pedagogical guide outlining common standards of training in March 2015 to ensure better cybersecurity awareness in SMEs. The guide outlines the minimum requirements for training and aims to create a contact person for cybersecurity (référent en cybersécurité) in SMEs. It requires a minimum of seven modules, giving an overview of the scope of cybersecurity, its legal foundations, its relevance within the general security model of a company, the current situation, as well as government institutions and groups that can be of help. This recently developed procedure has yet to produce a review of individuals and SMEs that have taken part in it.

2.2.4 Manager and decision-making level training

A more general challenge, also striking large corporations and CI operators, as well as public institutions, is that IT governance and cybersecurity are often left at the subaltern level of corporate management, with little interaction with the rest of the business structure in spite of the corporation's ever increasing reliance on IT. There is a gap in cybersecurity competences at senior executive and decision-making level – the competences which stretch beyond technical knowledge into business, economy, law and regulation, international relations, psychology, and public relations. The lack of multidisciplinary competences at the managerial level puts the companies and institutions, including CI, in an increasingly inferior position to cyber-attackers.

A number of governments have taken strategic steps to ensure that cybersecurity comes to the prime line of decision-making and business management in all sectors, especially with CI operators, through stimulating managerial-level training encompassing a variety of thematic areas. The Executive Academy that has been developed within the broader Israeli CyberSpark Initiative is likely the lead example. It's International School of Cyber Training for Senior Executives and Decision Makers that combines cutting-edge knowledge, best practices, lab experience, and simulations, while involving renowned lecturers from universities, the IT industry, and the governmental sector. Intensive 2-3-day programmes target corporate C-level executives, directors and board members, and governmental and public sector leadership and decision-makers, and are focused on practical knowledge covering a variety of thematic areas including technology and security angles, leadership skills, planning and decision-making, risk-management, strategic planning, human resources, legal environment, and marketing and communications.

Finland offers manager and decision-making level within the academic portfolio: a Master's degree in Cybersecurity in English is offered within a broader JyvSecTec framework, targeting national and international professionals who hold/will hold management positions in cybersecurity. The 60 European Credit Transfer System (ECTS) programme is part-time and requires two years of participation to complete, including one weekend per month of in situ participation.

The Korean Internet Security Agency (KISA) seeks to strongly promote the cybersecurity labour market by partnering with universities to create tailor-made programmes, with its Information Protection lecture tours for security managers in enterprises, and professional education for the diffusion of information protection knowledge. In France, in addition to the already mentioned référent en cybersécurité training which also argues for better IT governance and security, a group of IS managers have founded the Club des directeurs de sécurité des entreprises (CDSE) which is also working on cybersecurity. In Germany, a number of initiatives aimed at raising IS and cybersecurity awareness for managers have been grouped in the Deutschland sicher im Netz supported by the BMI as well as the ACS, and managed by BITKOM and the BSI. These measures are complementary to the ones already discussed within the collaboration with certification bodies.

Finally, some professional certification bodies have developed IT governance and cybersecurity frameworks. Among these, the Control Objectives for Information and Related

Illustration 8: Quick and applied cybersecurity training for the CEO and decision-making levels is critical, including aspects of technology, law, diplomacy, human resources, and communications.

Technology framework, COBIT 5.0, developed by ISACA, has received noticeable support by the NIST Framework for Improving Critical Infrastructure Cybersecurity in the USA. It aims to create a general governance plan for companies where IT is not confined to specialists but is rather a transversal theme. There is a general offer for boot camp training for managers in order to gain an understanding of the basic cybersecurity issues.

While these initiatives and study programmes are developing, they all require interest from the applicants and this may be seen as a potential gap in cybersecurity for the time being. The lack of awareness by the senior executive and the decision-making level diminishes the incentive to properly invest in the physical infrastructure and technical know-how and often depends on so-called trigger-events, such as large-scale security breaches with their consequences, before cybersecurity gains the recognition needed.

2.2.5 Knowledge frameworks, job descriptions and professionalisation of cybersecurity

An ongoing and heavy resource-consuming process is the development of descriptions of cybersecurity jobs, creating the knowledge frameworks, and shaping cybersecurity as a profession. Over the last 10-20 years, cybersecurity has become an overarching term for the many tasks, specialisations and jobs required to ensure IS on computer systems. This has led to a situation where it is difficult to assess what exactly it encompasses. Another issue countries have been facing is defining what it means to secure a system and what competences are needed in order to do so. Coupled with the fast evolution of the domain, this has been a major challenge that in some cases, such as in the USA, date back to the early 1970s.

In order to facilitate an overview, some countries with the size and correlating resources (FR, UK, US) have been developing frameworks of knowledge or to a lesser extent profession descriptions. The advantage of knowledge frameworks over professional job descriptions is that frameworks go into the detail of expected tasks and the knowledge required. This may allow better understanding of the job than a generic job title. It also allows for recombination of requirements in a domain that is still undergoing numerous changes.

The reasoning behind this work is manifold:
- Allows the elaboration of regulations and training.
- Envisions possible security loopholes.
- Assesses the required skills and competences.
- Attempts to create a common understanding between employers and potential employees.
- Stimulates public and student awareness by creating 'professions' that are then publicised as promising and attractive, thus driving a demand for education.

The most developed framework in both cases is the US model. The National Initiative for Cybersecurity Education (NICE) led by NIST has developed the National Cybersecurity Workforce Framework 2.0. The first version was published in 2013, and the second draft version in May 2014. It is the fruit of a long mapping process of knowledge, skills, and abilities (KSAs) done in collaboration with many federal institutions, as mentioned earlier. This catalogue breaks down potential jobs into approximately 30 specialty areas with their necessary KSAs for a particular task. By developing 'soft' standards on the cybersecurity workforce, it is creating an overview of cybersecurity roles and their respective KSAs and thus closing the gap between employers and jobseekers, as each party can get a better idea of what is expected. Breaking down the jobs into KSAs also allows for recombination in the case of evolution and tailoring for each company.

The publicly available framework is being used by the NSA/DHS in order to establish whether a university has met the required curricula standards for certification. It seems that one of the underlying factors is that the jobs and the requirements evolve on a regular basis. As a federal government initiative, the recent DoD 8410 Directive known as Information Assurance Workforce Improvement Program is also based on the framework. It can be expected that most US government jobs in cybersecurity may use this framework in the coming years and consequently create a standard between the public and private sector.

The recently launched UK initiative 'Inspired Careers' and the French ANSSI Job profile (profils métiers) initiative define a small set of jobs and expected activities descriptions, but are not as comprehensive and detailed as the US version, which is easier to tailor due to the detailed Knowledge, Skills and Abilities (KSA) and Knowledge Units (KU).

The use of such reference frameworks creates more awareness about the needs and required knowledge in the general public, but more importantly it allows HR personnel, who in many cases do not have the specific knowledge of cybersecurity, to better determine the competencies needed by the employer and those offered by the potential candidates, and thus hire the right personnel. This is an ongoing development where new jobs, in the sense of competences not recognised before, are being created and defined. It remains to be seen how this development will affect academia in general, but more specifically the certification companies in the medium to long run.

Illustration 9: A lack of common understanding of what are (and will be) cybersecurity competences demands that both the tasks and the required knowledge be defined, to help employers and employees.

3 Conclusion

Cybersecurity has come to the forefront of the political and diplomatic agenda due to the increasing risks for fundamental functioning of the societies. At the same time, it is creating potential for economic growth through the development of new markets and industries, such as hardware and software solutions, cybersecurity insurance, as well as education and research. The studied OECD countries seem to have recognised both sides of this coin, and are exploring different ways to increase cybersecurity competences within both the public and the private sector. This report has identified a number of trends which contribute to transforming labour markets – increasing the cyber-preparedness of institutions, companies and CI, but at the same time preparing the countries for global competitiveness in the cybersecurity industry.

The pace of development of technology and trends, as well as the multidisciplinary nature of the problem, require a comprehensive approach to developing competences with professionals in CI operators, industry, and government services that goes beyond traditional education and simple training for institutions and companies. The experiences from the studied countries show that a short-term response to demands for quality labour is in professional training targeting technology and IT specialists in public and private sectors, mainly delivered in cooperation with the private certification and training institutions which have cutting-edge knowledge. Equally important is targeting the chief executive and decision-making-level professionals, mainly through multidisciplinary programmes delivered at universities but shaped through a public-private partnership.

A long-term response appears to be in building on economic potentials rather than risks, and strengthening educational and research institutions through cooperation of authorities, industry, and the academic sector. The most remarkable trend, evident in most of the countries studied, is the development of regional education and research hubs, technology incubators, and start-ups at established universities and with funding from the ICT industry – often in places close to the security services or related authorities. Such initiatives bring direct benefits to universities, companies, and the public sector, contribute to transforming the labour markets, and position countries in the global race for cybersecurity industry dominance.

At the same time, partnerships between governments and the professional training and certification industry enables shaping of the proper regulatory environment for cybersecurity, and making the certification requirements and training offers for the public and the private sector compatible, thereby allowing for rapid labour market qualification and conversion. Not least, several notable attempts are being made to professionalise cybersecurity by defining job descriptions and, more importantly, creating knowledge frameworks which should allow for re-shaping the formats of labour supplies according to dynamic demands of cyber-reality.

While there was no specific trend identified for CI security, it is evident that this aspect is present in almost all the trends. CI is increasingly operated by the private sector which is in focus of many of the identified trends. Other trends address the compatibility between cybersecurity certification and requirements within the corporate sector – especially the SMEs – which serve as suppliers to the public institutions and the CI operators. Several trends focus on the preparedness of the public sector, which is of direct importance for the security of CI. Finally, long-term initiatives, such as PPP-based regional developments, provide a sustainable supply of qualified labour – technical, managerial and senior-level staff – for industry as well as for critical and security sectors.

Finally, it is important to underline that all the policy options identified in this report involve partnerships, mainly in the form of a strategy lead by government; funding and cutting-edge experience from the corporate sector, especially large corporations and the IT industry; and the research and knowledge incubator potentials of the universities. Each party has an interest in strengthening local expertise instead of, or at least along with, involving expertise from abroad, which creates a stimulus for PPP on all sides.

The identified trends in the selected 10 OECD counties can serve as policy options for strengthening cybersecurity skills and competences in Switzerland, including those significant for CI protection.

4 References

Books and papers

Brunner EM and Suter M (2008) *International CIIP Handbook 2008/2009.* In: CRN Handbooks 4(1). ETH Zurich: Center for Security Studies. Available at http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=91952

Gelbstein E (2015) *Cybersecurity: What we (may not) know we (do not) know – An overview of the cybersecurity challenge.* The Geneva Internet Platform. Available at http://giplatform.org/sites/default/files/GIP%20Background%20document%20-%20An%20overview%20of%20the%20cybersecurity%20challenge.pdf

Glaser G B and Strauss L A (2008) *The Discovery of Grounded Theory: Strategies for Qualitative Research.* London: Aldine Transaction, 2008 [1st ed. 1967].

Libicki M C, Senty D and Pollak J (2014) *Hackers wanted: an examination of the cybersecurity labor market.* RAND Corporate. Available at http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

Radunović V (2013) *DDoS – Available Weapon of Mass Disruption.* Proceedings of the 21st Telecommunications Forum (TELFOR), pp.5-9.

SDC (2006) *Capacity Development in SDC.* SDC Working Paper, Bern 2006. Available at https://www.eda.admin.ch/content/dam/deza/en/documents/die-deza/strategie/202114-capacity-development-sdc_EN.pdf

Other web-based sources

Note: All sites were last accessed 24 November 2015

Booz Allen Hamilton – Economist Intelligence Unit (2011) 'Cyber Power Index.' Available at http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

European Commission (ND) 'EU FP7 Seventh Framework Programme for Research.' Available at http://ec.europa.eu/research/fp7/index_en.cfm

International Telecommunications Union-ABI Research (2014) 'Global Security Index and Cyberwellness Profiles Report.' Available at http://www.itu.int/pub/D-STR-SECU-2015

Security Defence Agenda (Friends of Europe) (2012) 'Cyber-security: the vexed questions of global rules.' Available at http://www.friendsofeurope.org/security-europe/3110/

Country-based references

Austria

Critical Information Infrastructures Protection approaches in EU: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf

Bundeskanzler Amt. 'Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP).' 2014. https://www.bka.gv.at/DocView.axd?CobId=58907

Bundeskanzler Amt. 'Austrian Cyber Security Strategy.' 2013. https://www.bka.gv.at/DocView.axd?CobId=50999

Bundeskanzler Amt. 'Österreichisches Informationssicherheitshandbuch 4.0.' 2014. https://www.sicherheitshandbuch.gv.at/2013/downloads/sicherheitshandbuch.pdf

Bundeskanzler Amt. 'National ICT Security Strategy Austria.' 2012. http://www.oesterreich.gv.at/DocView.axd?CobId=48411

Austrian Computer Society https://www.ocg.at/en/history

Austrian Internet Security Platform https://www.onlinesicherheit.gv.at/

Austrian Institute of Technology http://www.ait.ac.at/

SBA Research https://www.sba-research.org/

Cybersecurity Challenge Austria http://www.cybersecuritychallenge.at/

Cooperation Open Government Data Austria https://www.data.gv.at/infos/cooperation-ogd-austria/

Internet Offensive Österreich http://www.internetoffensive.at/

European Commission. 'e-skills in Europe: Austria Country Report.' 2014. http://ec.europa.eu/DocsRoom/documents/4562/attachments/1/translations/en/renditions/pdf

Estonia

Estonian Information Technology College http://www.itcollege.ee/en/

HITSA (Hariduse Infotehnoloogia Sihtasutus) Innovation Centre
http://www.innovatsioonikeskus.ee/en

HITSA. 'Strategy for 2014-2020.' 2014.
http://www.hitsa.ee/files/HITSA_strategy_2020.pdf

Estonian Defence League Cyber Unit
http://www.kaitseliit.ee/en/edl

NATO Cooperative Cyber Defence Centre of Excellence. 'The Cyber Defence Unit of the Estonian Defence League.' 2013.
https://ccdcoe.org/multimedia/cyber-defence-unit-estonian-defence-league-legal-policy-and-organisational-analysis-0.html

Ministry of Foreign Affairs of the Republic of Estonia. 'U.S. Estonian Cyber Partnership Statement.' 2013.
http://vm.ee/sites/default/files/content-editors/S-Estonian%20Cyper%20Partnership%20Statement.pdf

Ministry of Economic Affairs and Communications
https://www.mkm.ee/en/objectives-activities/information-society/cyber-security

Ministry of Economic Affairs and Communications. '2014-2017 Cyber Security Strategy.'
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf

European Commission. 'e-skills in Europe: Estonia Country Report.' 2014.
http://ec.europa.eu/DocsRoom/documents/4568/attachments/1/translations/en/renditions/native

Government of Estonia. 'National Reform Program 'Estonia 2020.' 2011.
http://ec.europa.eu/europe2020/pdf/nrp/nrp_estonia_en.pdf

Tehnopol
http://www.tehnopol.ee/?lang=en

Finland

Information Society Code
http://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf

DIGILE
http://digile.fi/en/

SHOK
http://www.shok.fi/en/shok-in-english/JyvSecTec
http://jyvsectec.fi/en/

JAMK University of Applied Sciences Master's Degree in Cybersecurity:
http://www.jamk.fi/en/Education/Technology-and-Transport/Information-Technology-Masters-Degree/

Tekes: Finish Funding Agency for Innovation
https://www.tekes.fi/en/

Cybersecurity Finland
http://www.cyberfinland.fi/en/

Finnish Information Security Cluster
http://www.fisc.fi/en/
Inforte.fi
http://inforte.jyu.fi/

The Security Committee. 'The Implementation Programme for Finland's Cyber Security Strategy.' 2014.
http://www.turvallisuuskomitea.fi/index.php/en/component/k2/39-the-implementation-programme-of-the-cyber-security-strategy

Ministry of Defence. 'Cyber Security Strategy.' 2013.
http://www.defmin.fi/en/publications/strategy_documents/finland_s_cyber_security_strategy

Security in Society. 'Finland´s cyber security strategy – Background dossier.' 2013.
http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/48-finlandas-cyber-security-strategy-background-dossier

Security in Society. 'Security Strategy for Society.' 2010.
http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/26-security-strategy-for-society

France

ANSSI
http://www.ssi.gouv.fr/

ANSSI – Centre de Formation à la Sécurité des Systèmes d'Information (CFSSI)
http://www.ssi.gouv.fr/particulier/formation/

ANSSI – CFSSI – Profils métiers
http://www.ssi.gouv.fr/particulier/formation/profils-metiers-de-la-cybersecurite/

Délégation Interministérielle à l'Intelligence Economique (D2IE). 'Formation à la cybersécurité des TPE et des PME: Référentiel pédagogique.' 2015.
http://www.intelligence-economique.gouv.fr/sites/default/files/d2ie_formation_cybersecurite_des_tpe_pme_mars20152_0.pdf

Invest in Bretagne – Pôle d'excellence cyber
http://www.invest-in-bretagne.org/-la-bretagne-reference-nationale-en,409-.html

ANSSI. 'Label France Cybersecurity – Press release.' 2015.
http://www.ssi.gouv.fr/publication/nouvelle-france-industrielle-axelle-lemaire-remet-les-premiers-labels-france-cybersecurity-a-loccasion-de-ledition-2015-du-forum-international-de-la-cybersecurite/

Club des Directeurs de Sécurité des Entreprises (CDSE)
https://www.cdse.fr/-cdse-

ANSSI – Formation en Expert en Sécurité des Systèmes d'Information (ESSI)
http://www.rncp.cncp.gouv.fr/grand-public/visualisationFiche?format=fr&fiche=4245

La Commission du Livre Blanc. 'Livre blanc sur la défense et la sécurité nationale.' 2013.
http://www.livreblancdefenseetsecurite.gouv.fr/index.html

ANSSI. 'Information systems defence and security strategy.' 2011.
http://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/

Germany

IT-Security Law
http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1447686734414

BMBF Cybersecurity Research Program
https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html

Center for IT-Security, Privacy, and Accountability (CISPA)
http://cispa.saarland/

Max Planck Institute for Software Systems
https://www.mpi-sws.org/index.php

German Research Center for Artificial Intelligence
http://www.dfki.de/web?set_language=en&cl=en

Max-Planck Institute for Informatics
http://www.mpi-inf.mpg.de/home/

European Center for Security and Privacy by Design in Darmstadt (EC-SPRIDE – CASED)
https://www.cased.de/en/research/ecspride.html

Technical University Darmstadt
http://www.tu-darmstadt.de/

Center for Advanced Security Research Darmstadt (CASED)
https://www.cased.de/en.html

Fraunhofer Institute for Secure Information Technology
https://www.sit.fraunhofer.de/en/

Competence Center for Applied Security Technology (CAST)
http://www.cast-forum.de/en/home.html

KASTEL – Competence Center for Applied Security Technology in Karlsruhe (KIT)
https://www.kastel.kit.edu/

Kompetenz- und Forschungszentren für IT-Sicherheit (regrouping CISPA, EC-SPRIDE and KASTEL)
http://www.kompetenz-it-sicherheit.de/

Software Cluster Germany
http://www.software-cluster.com/de/

IT-Sicherheit in der Wirtschaft (Federal Ministry for Economic Affairs and Energy)
http://www.it-sicherheit-in-der-wirtschaft.de/

Deutschland Sicher im Netz (Federal Ministry of the Interior)
https://www.sicher-im-netz.de/

IT @ Mittelstand (FMI with support of the FMEAE)
https://www.sicher-im-netz.de/it-sicherheit-mittelstand

Open Competence Center for Cybersecurity
https://www.open-c3s.de/startseite_open-c3s.html

Allianz für Cybersicherheit (Federal Office for Information Security)
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html

Cybersecurity Practitioner
http://www.isaca.de/index.php/zert-start/zertifikate/cybersecuritypractitioner

Bitkom Akademie
https://www.bitkom-akademie.de/seminare

Israel

CyberSpark Initiative
http://www.cyberspark.org.il/

CyberSpark Executive Academy
http://www.cyberspark.org.il/#!executive-academy/c1wgl

Cyber at the Ben-Gurion University of the Negev
http://in.bgu.ac.il/en/cyber/Pages/default.aspx

Homeland Security Institute at Ben-Gurion University of the Negev
http://in.bgu.ac.il/en/hsi/Pages/mission.aspx

Tel Aviv University – Blavatnik Interdisciplinary Cyber Research Center (ICRC)
https://icrc.tau.ac.il/

Shamoon College of Engineering – Cyber Operations (Cyber OPs)
http://www.sce.ac.il/cyber/

Prime Minister's Office Decision to Establish a New National Authority for Operative Cyber Defense
http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokecyber2210914.aspx

The 'Magshimim Leumit' Program
http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Magshimim%20Leumit%20program.pdf

Republic of Korea

Korean Internet Security Agency (KISA)
http://www.kisa.or.kr/eng/main.jsp

Korea University Graduate School of Information Security
http://kuweb.korea.ac.kr/imeeng/
http://koreauniv.pure.elsevier.com/en/organisations/graduate-school-of-information-security%2804781502-ca44-44c3-b73a-311207f9df41%29.html

Korea University, Department of Cyber Defense Information Security
http://graduate.korea.ac.kr/DATA/univManage/97/20140226140459.pdf (page 9)
http://graduate.korea.ac.kr/department/univManage/data.jsp?idx=97

Korea Advanced Institute of Science and Technology (KAIST) Graduate School of Information Security
http://gsis.kaist.ac.kr/

Korea National Defense University
https://www.kndu.ac.kr/eng/

Sogang University Graduate School on Information Technology
http://www.sogang.ac.kr/english/academic/04_graduate_0405.html

Cyber University of Korea, Department of Information Management and Security
http://eng.cuk.edu/100531.do

2013 Korea Internet Whitepaper, KISA
http://isis.kisa.or.kr/eng/ebook/EngWhitePaper2013.pdf

The Netherlands

Ministry of Security and Justice, National Cyber Security Centre. 'National Cyber Security Strategy 2: From awareness to Capability.' 2015
https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html

The Hague Security Delta (HSD)
https://www.thehaguesecuritydelta.com/

Cyber Security Academy (CSA)
https://www.csacademy.nl/en/about-csa

The HSD Education Platform
http://www.hsa.counterpoint.co.nl/

Black Hat Europe
https://www.blackhat.com/eu-15/

Dutch CyberSecurity Research and Education Platform
http://www.nwo.nl/en/news-and-events/news/2015/ew/new-dutch-cybersecurity-research-and-education-platform.html

The HITB (Hack In The Box) SecConf
http://conference.hitb.org/hitbsecconf2016ams/

United Kingdom

National Audit Office. 'Update on the National Cyber Security Programme.' 2014
https://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme.pdf

Department for Business, Innovation and Skills. 'UK Cyber Security Standards.' 2013
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf

Department for Business, Innovation and Skills. 'Developing our capability in cyber security: Academic Centres of Excellence in Cyber Security Research.' 2014.
http://dera.ioe.ac.uk/19756/

Department for Business, Innovation and Skills, Pwc. 'UK CYBER SECURITY STANDARDS Research Report.' 2013.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf

Cabinet Office. 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.' 2011.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Cabinet Office. 'The UK Cyber Security Strategy: Report on Progress and Forward Plans.' 2014.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

Cyber Essentials, CREST
http://www.cyberessentials.org/

Cyber essentials scheme: overview, The Department for Business, Innovation and Skills (BIS)
https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

GCHQ. 'Developing the Cyber Experts of the future – GCHQ certifies Master's Degrees in Cyber Security.' 2014
http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-certifies-Masters-Degrees-in-Cyber-Security.aspx

GCHQ Certification of Master's degrees in Cyber Security
https://www.cesg.gov.uk/awarenesstraining/academia/Pages/Masters-Degrees.aspx

Academic Centres of Excellence in Cyber Security Research
https://www.epsrc.ac.uk/research/centres/acecybersecurity/

Institute of Information Security Professionals (IISP)
https://www.iisp.org

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

Inspired Careers
http://www.inspiredcareers.org

United States

The White House. 'The Tech Hire Initiative.' 2015.
https://www.whitehouse.gov/the-press-office/2015/03/09/fact-sheet-president-obama-launches-new-techhire-initiative

National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD), NSA
https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

SEAL Program, National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD), NSA
https://www.nsa.gov/ia/academic_outreach/nat_cae/seal_program.shtml

National IA Education & Training Programs (NIETP), Information Assurance Directorate (IAD), NSA
https://www.iad.gov/NIETP/aboutCAE.cfm

The White House. 'Executive Order 13636.' 2013.
https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

NIST. 'Framework for Improving Critical Infrastructure Cybersecurity.' 2014.
http://www.nist.gov/cyberframework/

NICE: National Initiative for Cybersecurity Education
http://csrc.nist.gov/nice/

The White House. 'Comprehensive National Cybersecurity Initiative.' 2009.
https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Congress. 'Federal Information Security Management Act.' 2002.
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Congress. 'Federal Information Security Modernization Act (FISMA).' 2014.
http://www.dhs.gov/federal-information-security-management-act-fisma

Committee on Nation Security Systems (CNSS)
https://www.cnss.gov/CNSS/index.cfm

CNSS. 'CNSS Report: Progress Against 2008 Priorities.' 2009.
https://www.cnss.gov/CNSS/issuances/CNSS_Reports.cfm

CNSS. 'NSTISSI No. 4011: National Training Standard for Information Systems Security (INFOSEC) Professionals.' 1994.
https://www.cnss.gov/CNSS/openDoc.cfm?XTKaEwRECBEVILnlxPQAPg==

CNSS. 'CNSSI No. 4012 National Information Assurance Training Standard for Senior Systems Managers.' 2004.
https://www.cnss.gov/CNSS/openDoc.cfm?NgkabhsrhhWGSzodEPRy4Q==

CNSS. 'CNSSI No. 4013 National Information Assurance Training Standard For System Administrators (SA).' 2004.
https://www.cnss.gov/CNSS/openDoc.cfm?vBaZlTmIOm8rkTMRYV/WhA==

CNSS. ' CNSSI No. 4014 Information Assurance Training Standard for Information Systems Security Officers.' 2004.
https://www.cnss.gov/CNSS/openDoc.cfm?yOcso8HUsc63UbiVt3RYMg==

CNSS. ' NSTISSI No. 4015 National Training Standard for Systems Certifiers.' 2000.
https://www.cnss.gov/CNSS/openDoc.cfm?Wt/7JvRYADwh3yDLcqb+fA==

CNSS. ' CNSSI No. 4016 National Information Assurance Training Standard For Risk Analysts.' 2005.
https://www.cnss.gov/CNSS/openDoc.cfm?teuaswXATKFSd3qr8YgYPA==

American National Standards Institute
http://www.ansi.org/

Navy COOL Information Assurance Technician Flow Chart
https://www.cool.navy.mil/usn/ia_documents/ia_iat_flow.htm

Navy COOL Information Assurance Manager Flow Chart
https://www.cool.navy.mil/usn/ia_documents/ia_iam_flow.htm

National Cybersecurity Center of Excellence (NCCoE), NIST
http://nccoe.nist.gov/content/about

Critical Infrastructure Cyber Community C^3 Voluntary Program
http://www.dhs.gov/ccubedvp

National Initiative for Cybersecurity Careers and Studies (NICCS)
https://niccs.us-cert.gov/

NICE. 'National Cybersecurity Workforce Framework 2.0.' 2015.
https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework

Professional certification bodies

Note: *List includes bodies encountered during research. It is a non-exhaustive list.*

CompTIA:
https://www.comptia.org/

CREST (Council of registered ethical security testers):
http://www.crest-approved.org

EC-Council:
http://www.eccouncil.org/

Global Information Assurance Certification (GIAC)-(Certifications developed by SANS):
http://www.giac.org/

(ISC)2:
https://www.isc2.org/aboutus/default.aspx

ISACA:
http://www.isaca.org/about-isaca/Pages/default.aspx

ISACA Germany Chapter e.V. :
http://www.isaca.de/

Mile2:
http://mile2.com/

Offensive Security:
https://www.offensive-security.com/

SANS:
https://www.sans.org/about/

Annex: Acronyms

ABI	Allied Business Intelligence
ACE	Academic Centre for Excellence
ACS	The Alliance for Cybersecurity
AIT	Austrian Institute for Technologies
ANSSI	French Network and Information Security Agency
APMG	Accrediting Professional Managers Globally
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BMBF	German Ministry of Education and Research
BMI	Ministry of the Interior
BMWi	Federal Ministry for Economic Affairs and Energy
BSI	Federal Office for Information Security of Germany
CAE	Center for Academic Excellence in Information Assur ance Education
CAE-IAE	Center for Academic Excellence in Information Assurance Education
CCP	CESG Certified Professional
CCT	CESG Certified Training
CDSE	Club des directeurs de sécurité des entreprises
CCDCoE	Cooperative Cyber Defence Centre of Excellence
CEO	Chief Executive Officer
CESG	Communications-Electronics Security Group
CFSSI	Centre de formation à la sécurité des systèmes d'information
CI	Critical infrastructure
CNSS	Committee on National Security Systems
COBIT	Control Objectives for Information and Related Technology
COMET	Competence Centre for Excellent Technologies
CompTIA	Computing Technology Industry Association
CREST	Certificateless Registry for Electronic Share Transfer
D2IE	Delegation on Economic Intelligence
DHS	Department of Homeland Security
DoD	Department of Defense
EC-Council	The International Council of Electronic Commerce Consultants
ECTS	European Credit Transfer System
ESSI	European Strategic Safety Initiative
EU	European Union
FDFA	Federal Department of Foreign Affairs
FFG	Austrian Research Promotion Agency
G20	Group of 20 (Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, México, Russia, Saudi Arabia, South Africa, Korea, Turkey, the United Kingdom, United States and European Union)
GCHQ	Government Communications Headquarters
HITSA	Information Technology Foundation for Education
HR	Human resources
IA	Information Assurance
IAM	Information Assurance Management
IAT	Information Assurance Technical
INCB	Israel National Cyber Bureau
ISACA	Information Systems Audit and Control Association
(ISC)²	The International Information Systems Security Certification Consortium
IS	Information security
IS/IA	information security and information assurance
IT	Information Technology
ITU	International Telecommunication Union
JAMK University	Jyväskylän ammattikorkeakoulu
JyvSecTec	Jyväskylä Security Technology
KAIST	Korea Advanced Institute of Science and Technology
KISA	Korean Internet Security Agency
KSA	Knowledge, Skills and Abilities
KU	Knowledge Units
NATO	North Atlantic Treaty Organization

NATO CCDCoE	NATO Cooperative Cyber Defence Centre of Excellence
NCS	National Strategy for the Protection of Switzerland against Cyber Risks
NICE	National Initiative for Cybersecurity Education
NIETP	National IA Education & Training Programs
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
PPPs	public private partnerships
SCADA	supervisory control and data acquisition
SDC	Swiss Agency for Development and Cooperation
SEAL	Security Education Academic Liaison
SHOK	Strategic Centres for Science, Technology, and Innovation in Internet economy
SME	small and medium enterprise
RAND Corporation	Research And Development Corporation
R&D	research and development

This report is available at: **www.diplomacy.edu/cybersecurity**

About the authors

Vladimir Radunović

Vladimir Radunović is a director of e-diplomacy and cybersecurity educational and training programmes and a lecturer at DiploFoundation. He holds an MSc in electrical engineering from the University of Belgrade and a Master degree in contemporary diplomacy from the University of Malta with thesis on e-diplomacy, and has undertaken a PhD programme in cybersecurity. Vladimir was born and lives in Serbia. He can be contacted at vladar@diplomacy.edu

David Rüfenacht

David Rüfenacht works on a consultancy basis for the Geneva Internet Platform. He has worked as a social researcher and project manager in various domains but has a keen interest in the social and political impacts of internet, particularly of cybersecurity and the implications of 'big data' as an internet user. David holds a MA in International Relations and a MA in Social Anthropology. He can be contacted at davidr@diplomacy.edu

About DiploFoundation

DiploFoundation is a leading global capacity development organisation in the field of Internet governance.

Diplo was established by the governments of Switzerland and Malta with the goal of providing low cost, effective courses and training programmes in contemporary diplomacy and digital affairs, in particular for developing countries. Its main thematic focuses are on Internet governance (IG), e-diplomacy, e-participation, and cybersecurity.

Diplo's flagship publication 'An Introduction to Internet governance' is among the most widely used texts on IG, translated into all the UN languages and several more. Its online and in situ IG courses and training programmes have gathered more than 1500 alumni from 163 countries. Diplo also hosts the Geneva Internet Platform (GIP).

Diplo also provides customised courses and training both online and in situ.

DIPLO FOUNDATION
Malta: Anutruf, Ground Floor, Hriereb Str, Msida, MSD 1675, Malta
T. +356 21 333 323, F. +356 21 315 574
Geneva: Rue de Lausanne 56, CH-1202 Geneva, Switzerland
T. (41) 22 741 0420; F. (41) 22 713 1663
E-mail: ig@diplomacy.edu www.diplomacy.edu/cybersecurity