Executive summary

Research commissioned by the Federal Department of Foreign Affairs of Switzerland

Vladimir Radunović and David Rüfenacht
DiploFoundation
February 2016
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. Developing knowledgeable and competent labour for this fast-changing area is one of the main strategic challenges faced by many countries.

DiploFoundation report Cybersecurity Competence Building Trends 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, Estonia, Finland, France, Germany, Israel, the Netherlands, the Republic of Korea, the United Kingdom, and the United States.

Drivers of change: risks and opportunities

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 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.

Cybersecurity Competence Building Trends 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.

This illustrated executive summary presents key identified trends.

For more information and specific examples on each trend, a reference to the chapter in the full report can be found next to this icon 📚.

The full report is available at: www.diplomacy.edu/cybersecurity
Comprehensive approach: public-private partnerships

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.

DiploFoundation @DiplomacyEdu Mar 28
Building #cybersecurity competences powered by risks & opportunities, requires cooperation by governments, business & academia
Long-term effects: strengthening university curricula & research capacities through financial support by the public & private sector.
Key cybersecurity competence building trends

University programmes supported by the government

All of the countries explored 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. ☞ [Report p.12]
Developing a #cybersecurity industry through innovation hubs at universities strengthens competences & global competitiveness.
Reaping the economic potentials: regional development

Major 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. 📃[Report p.15]
Labelling of universities

Some university training facilities tend to also have partnerships with state security institutions as in cases of the UK, the US, 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, critical infrastructure operators, or the private sector which intends to provide services to the government. The UK and the US have taken an additional step in developing a university labelling programme which aims to encourage academic institutions to include specific knowledge in their curricula. [Report p.13]
Collaboration with professional certification bodies

While approaches to strengthening academic programmes 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 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. [Report p.18]

DiploFoundation @DiplomacyEdu
Governments can cooperation w/ professional certification bodies to create certificates adjusted to national environment & needs
State personnel training through professional certification bodies encourages workforce mobility; in-house training enhances control.
State personnel training

The approaches by governments range from requiring certificates from private certification institutions for government or private sector employment, such as in the US, to developing their own certification programmes in collaboration with such a private certification institution, such as in Germany. Engaging professional certification bodies for state personnel training, such as in the UK or in the US, reduces the costs and encourages workforce mobility, while in-house training, such as in France, brings greater control and specialised focus. [Report p.16]
Improving the competences of the private sector

Several trends have identified the need for small and medium enterprises (SMEs) as well as critical infrastructure (CI) operators to grasp the stakes at hand and develop their competencies in the cyber realm. The UK has developed its Cyber Essentials toolkit for SMEs and requires its providers to adopt it, whereas in Germany and France initiatives were developed to support SMEs and critical infrastructure operators in increasing their cybersecurity. The US has developed a flexible Framework for Improving Critical Infrastructure Cybersecurity that companies of different size should be able to adopt. [Report p.19]
Cybersecurity in many organisations is affected by a ‘digital divide’ between ICT departments and decision makers, managers and senior executives. Two countries at the forefront of cybersecurity - Finland and Israel - have developed university-grade degrees and executive academic programmes in order to overcome this divide that exists in both private and public sectors. Germany uses an extensive professional network in order to push for manager awareness. [Report p.20]
Knowledge frameworks, job descriptions and professionalisation of cybersecurity

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 US has defined the required knowledge training for different jobs in its National Cybersecurity Workforce Framework 2.0. [Report p.21]
Cybersecurity as a driving force for the transformation of the national labour market
The effects of the trends identified in the study go 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.

The identified trends in the selected ten OECD counties can serve as policy options for strengthening national cybersecurity skills and competences, including those significant for critical infrastructure protection.

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.
## Overview of the most prominent examples from the studied countries

<table>
<thead>
<tr>
<th>STRENGTHENING ACADEMIC PROGRAMMES</th>
<th>University programs supported by the government</th>
<th>Labelling of universities</th>
<th>Regional development</th>
<th>State personnel training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Centres (Germany)</td>
<td>Center for Academic Excellence in Information Assurance Education (CAE) (United States of America)</td>
<td>Pôle d’Excellence Bretagne (France)</td>
<td>State Cantered Model: Expert en sécurité des systèmes d’information (ESSI certificate by ANSSI-CFSSI) (France)</td>
<td></td>
</tr>
<tr>
<td>JyvSecTec-JAMK (Finland)</td>
<td>Academic Centre for Excellence (ACE) (United Kingdom)</td>
<td>JAMK –JyvSecTec (Finland)</td>
<td>Private Sector training: US DoD Policy 8570.1 – 8410 with requirements for IA Technical and IA Management (United States of America)</td>
<td></td>
</tr>
<tr>
<td>KU Graduate School of IS and Department of Cyber Defense IS / KAIST Graduate School of IS (Republic of Korea)</td>
<td></td>
<td>The Hague Security Delta – Security Cluster (Netherlands)</td>
<td>CESG Certified Professional (United Kingdom)</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Hub within CyberSpark / 'Magshimim Leumit' advanced cybersecurity study programme (Israel)</td>
<td></td>
<td>Software Cluster Southwest Germany (Germany)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Technology Foundation for Education (HITSA) (Estonia)</td>
<td></td>
<td>NATO CCDCoE / e-Citizenship &amp; e-Government Initiatives (Estonia)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Austrian Institute for Technology and SBA Research (Austria)</td>
<td></td>
<td>CyberSpark Industry Initiative at Ben-Gurion University in Be’er Sheva (Israel)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CESG Certified Professional (United Kingdom)</td>
<td></td>
</tr>
<tr>
<td>State personnel training</td>
<td>Improving the competences of the private sector (SME and CI)</td>
<td>Manager and decision-making level training</td>
<td>Knowledge frameworks, job descriptions and professionalization</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>CNSS training requirements for professional training providers (United States of America)</td>
<td>'Framework for Improving Critical Infrastructure Cybersecurity' by NIST (United States of America)</td>
<td>Executive Academy within CyberSpark (Israel)</td>
<td>'National Cybersecurity Workforce Framework 2.0' by the National Initiative for Cybersecurity Education (NICE) (United States of America)</td>
<td></td>
</tr>
<tr>
<td>CESG Certified Professional requirements and Certified Training scheme (United Kingdom)</td>
<td>'Cyber Essentials' - standards/ requirements and Certification for SME (United Kingdom)</td>
<td>Master's degree in Cybersecurity at JyvSecTec (Finland)</td>
<td>'Inspired Careers' (United Kingdom)</td>
<td></td>
</tr>
<tr>
<td>BSI Cybersecurity Practitioner certificate with ISACA (Germany)</td>
<td>'IT Sicherheit in der Wirtschaft' with seminar 'IT-Sicherheit@Mittelstand' (Germany)</td>
<td>Korean Internet Security Agency (KISA) (Republic of Korea)</td>
<td>'Profils métiers' job profile by ANSSI (France)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Référent en cybersécurité' guide with standards by ANSSI and Inter-ministerial Delegation on Economic Intelligence - D2IE) (France)</td>
<td>Club des directeurs de sécurité des entreprises (France)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deutschland Sicher im Netz (Germany)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
DiploFoundation is a leading global capacity development organisation in the field of Internet governance and digital policy.

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 hosts the Geneva Internet Platform (GIP).

Diplo also provides customised courses and training both online and in situ, covering a wide range of subjects including cybersecurity, Internet governance, data protection and e-diplomacy.
DIPLO FOUNDATION

Malta: Anutzer, Ground Floor, Hriereb Str, Msida, MSD 1675, Malta
T. +356 21 333 323, F. +356 21 315 574

Switzerland: Rue de Lausanne 56, CH-1202 Geneva, Switzerland
T. (41) 22 741 0420; F. (41) 22 713 1663

Serbia: Diplo Centar, Gavrila Principa 44a, Beograd
T. +381 11 7614609; F. +381 11 7614701

e-mail: ig@diplomacy.edu

www.diplomacy.edu/cybersecurity