Cybersecurity Competence Building Trends

19 April 2016

Vladimir Radunović
DiploFoundation

David Rüfenacht
MELANI
**Context**

**Challenges**
- Threats to institutions, business, CI
- Multidisciplinary area (technology, law, diplomacy, economy, management, psychology, media)
- Fast-changing environment

**Opportunities**
- Driver for employment
- Economic growth
- Global competitiveness
Context

Developing national capacities and competences

BY

Transforming the national labour market to meet the changing environment

BUT

Building qualified labour goes beyond traditional education and one-off training courses
Research

- **Inquiry**: FDFA inquiry on ‘Promote cybersecurity competence building in Switzerland through lessons learned abroad’
- **Objective**: contribute to strengthening cybersecurity skills and competences in Switzerland (especially re. CI)
- **Task**: Review of trends and policy instruments of 10 OECD countries on cyber competence building that could feed into NCS
Methodology

- **Problem**: developing human skills and competences through training and education for technological and organisational measures to counter cyber-threats

- **Methodology**: Qualitative research (July-October 2015) based on review of the literature, content analysis of (open) documents, secondary analysis and statistics

- **Case selection**:
  - *Pre-set countries*: Estonia, Israel, Republic of Korea, the Netherlands, UK and US
  - *Added countries*: Austria, Finland, France and Germany
Key findings

- Countries observe both **risks and opportunities**: cyber-preparedness and global industry competitiveness

- Combination of **long-term and short-term** approaches to transforming labour markets

- Trends heavily based on **PPP** (development of curricula, certification, capabilities, regional hubs):
  - strategic lead and incentives by **government**
  - funds and cutting-edge technology by **private sector**
  - knowledge, outreach and research potential by **academia**
# Lead trends

## Promoting competence building at universities

<table>
<thead>
<tr>
<th>University programs supported by the government</th>
<th>Labelling of universities</th>
<th>Regional development</th>
</tr>
</thead>
</table>

## Competence building through professional training

<table>
<thead>
<tr>
<th>State personnel training</th>
<th>Collaboration w/ professional certification bodies</th>
<th>Improving the competences of the private sector (SME and CI)</th>
<th>Manager and decision-making level training</th>
<th>Knowledge frameworks, job descriptions and professionalization</th>
</tr>
</thead>
</table>
University programs supported by the government

• Strong PPP element
• Supported by government (specific Ministry)
• Economic growth is aimed
• Long term development
• Research Lab & Network development
University programs supported by the government
Labelling of universities

• Student advantage (tuition fees)
• University advantage (attract new students with image, potential facilitated research funding, research network, establishing programs)
• Government advantage (training for future employees, screening of future employees, potential say to research directions)
• Disadvantage: potential loss of independence and link with politics (real and/or reputational loss)

Example: Center for Academic Excellence in Defense Education (CAE-CD) (US)
Labelling of universities
Regional development

• Developing universities, research labs, innovation hubs, labs, joint ventures
• Need for funding: regional development and use of national and supra-national and/or research funding (especially private sector)
• Never a ‘totally’ new place: located in regions with lead universities and political and economic relevance
• Depends on context and geopolitical situation

Example: CyberSpark Industry Initiative at Ben-Gurion University in Be’er Sheva (Israel)
Regional development
State personnel training

Extremes: state training vs private training

- Government regulatory institution trains specialists:
  *Example*: ESSI certificate by ANSSI- CFSSI (France)
  - control, highly specialized
  - costly, high labor toll on regulatory institution, potentially longer to adapt, workforce mobility

- Use of professional certification bodies:
  *Example*: US DoD Policy 8570.1 – 8410 requirements (US)
  - low cost of adaption certification (technical experts), ‘soft’ standardization (public-private, national-international), workforce mobility, workforce reallocation time
  - takes time to decide on providers and/or certificates, costly for trainees (financial)
State personnel training

Professional Certification Body Dojo

Government Dojo
Collaboration with professional certification bodies

Creating a certificate for national needs

+ creates certificate adapted to national legal framework, advantages of professional certification bodies,

– needs national legal framework (takes time, commitment), suited for national not international, and need for ‘critical size’

*Example*: BSI Cybersecurity Practitioner (Germany)
Collaboration with professional certification bodies
Improving the competences of the private sector

- Especially for SME and CI
- Incident handling and prevention framework (using professional certification bodies)
- Frameworks and standards for private sector
- Government subcontractors mandated to implement
- Securing the chain
- Awareness training

*Example:* 'Cyber Essentials' - standards/requirements and Certification for SME (UK) & 'Référent en cybersécurité' guide with standards by ANSSI (France)
Improving the competences of the private sector
Manager and decision-making level training

- Addressing awareness among CEO & decision-makers
- Multidisciplinary: politics, regulation, business management
- Helps deciding on investments in IT and cybersecurity sectors in institutions
- Need for quick and applied training

*Example:* Executive Academy within CyberSpark (Israel) & Master’s degree in Cybersecurity at JyvSecTec (Finland)
Manager and decision-making level training
Knowledge frameworks and job descriptions

- Lack of understanding of what is and what will become cyber competence
- Defining tasks and required knowledge
- Allowing for recombination and evolution
- Helps employer, employee and HR for training management

Example: 'National Cybersecurity Workforce Framework 2.0' by the National Initiative for Cybersecurity Education (US)
Knowledge frameworks and job descriptions
Conclusion