ANALYSIS

EDUCATION AS A KEY FACTOR IN THE PROCESS OF BUILDING CYBERSECURITY

IZABELA ALBRYCHT

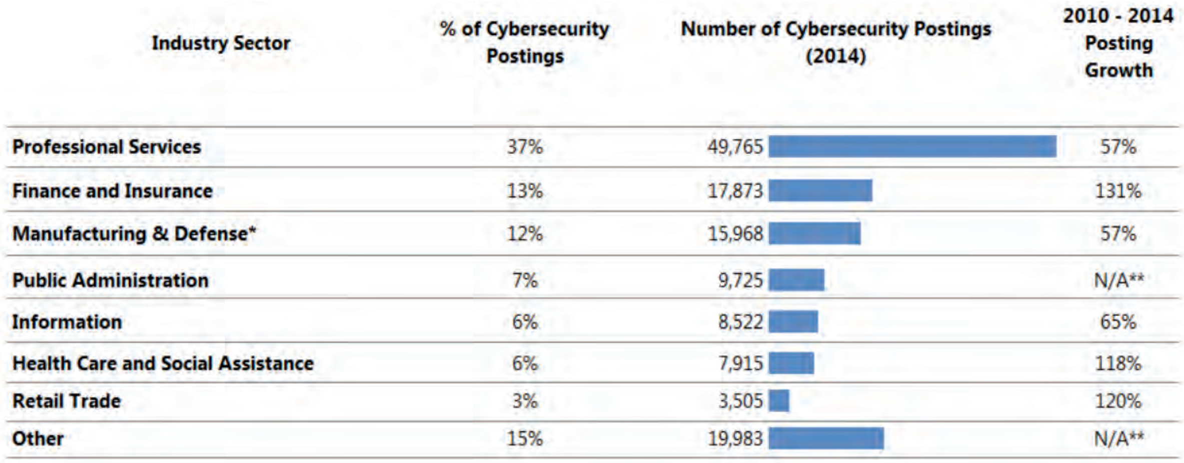
Izabela Albrycht is a Chairperson of the Board of the Kosciuszko Institute and the Chair of the CYBERSEC Organising Committee – annual public policy conference devoted to the strategic issues of cybersecurity. She is an author and co-author of publications focused on issues connected with international relations and EU Policies. She organises and co-organises research projects and conferences in Poland and abroad. She is the Editor Associate of the European Cybersecurity Journal and former Editor of the International Shale Gas & Oil Journal (2013-2014).

Over the last few decades, we moved a significant part of our multidimensional activities to the cyberspace. Aside from the obvious benefits, this process poses a huge risk for the entire civilization. The number of hacker attacks, implementations of information systems, as well as risks associated with the operation of cyberworld is rapidly increasing. In building cybersecurity we cannot sacrifice the benefits of digital, crosslinked and automatised reality. We need to catch up with "the bad guys." To do so, we dramatically need cybersecurity specialists. This need is reflecting in growing demand for cybertalents – highly qualified cyber personnel who will be able to respond to the increasingly sophisticated forms of cyberattacks (cybersecurity IT specialists) and who will be responsible for creating the architecture of cybersecurity (i.a. lawyers, political scientists, administration employees). Therefore, the key factor in the process of providing cybersecurity in public and private sectors is to adapt the education system this new long-term challenges as well as to the market needs to educate more and more cyberspecialists. It is not possible today to fill the ever-growing gap in employment in the ICT sector, neither the education of specialists who would be responsible for adapting the legislation and institutions of state in cybersecurity or for building international co-operation in this area.

The cybertalents' gap

There is a need for IT security specialists everywhere. Without them companies expose themselves to a multimillion loss, arising from incidents on the network. This high demand for cybertalents also occurs in companies in the critical infrastructure sector, banks, defence, professional service centres and automated industries and manufacturing (Table 1). It is a particularly important issue as cyberattacks on critical infrastructure facilities endanger national security and can be elements of both the classic and the hybrid form of war.

Table 1. Cybersecurity Demand Grows by Industry Sectors



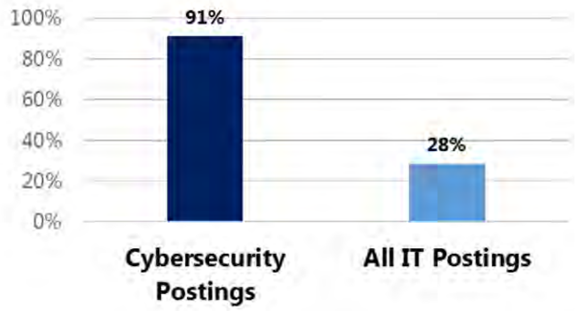
Industry Sector	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)	2010 - 2014 Posting Growth
Professional Services	37%	49,765	57%
Finance and Insurance	13%	17,873	131%
Manufacturing & Defense*	12%	15,968	57%
Public Administration	7%	9,725	N/A**
Information	6%	8,522	65%
Health Care and Social Assistance	6%	7,915	118%
Retail Trade	3%	3,505	120%
Other	15%	19,983	N/A**

Source: Job Market Intelligence: Cybersecurity Jobs, Burning Glass Technologies

The shortage of IT workers for example in Poland is very high and is up to 40 thousand people. In the entire European Union – according to the data published by the European Commission – the demand for professional ICT workers in the IT sector across many sectors in Europe is growing at a rate of approx. 3% annually despite the crisis[1] while the number vacancies for computer scientists can currently reach up to 300 thousand, and it could be up to 825,000 unfilled vacancies for ICT professionals by 2020[2].
In order meet this challenge the European Commission is leading a multi-stakeholder partnership, the Grand Coalition for Digital Jobs, aimed at tackling the lack of digital skills in Europe and the thousands of unfilled ICT-related vacancies across all industry sectors. The subject of digital skills gaps was discussed by Member States not later than December 11th by the EU ministers. According to the press release their objective is prepare the ground for a joint commitment to develop adequate levels of digital skills in the EU in the face rapid digitisation. In 2016, the Commission will present a comprehensive skills agenda[3].

According to Symantec, which is one of the chief market leaders, until 2019, the demand for specialists in cybersecurity could rise to approx. 6 million people worldwide[4]. This number includes 1.5 million new posts to be created within the next three years. This tendency is also confirmed in a recent report of another huge IT company, Cisco.[5]

Table 2. Growth in Job Postings.



Source: Job Market Intelligence: Cybersecurity Jobs, Burning Glass Technologies

> “The shortage of IT workers for example in Poland is very high and is up to 40 thousand people.

In turn, according to the report "Job Market Intelligence: Cyber Security Jobs, 2015,"[6] last year, 238 thousand job advertisements appeared in the US related to cybersecurity. In this field, positions for professionals make up 11% of all jobs in IT sector in the United States. Since the supply is not keeping pace with the demand (in 2010-2014 the employment of cybersecurity professionals has increased by as much as 91%!), wages are higher by an average of 9 % than in the entire industry (Table 2, Table 3).

It is not just a temporary trend. This is a long-term change, which requires wise strategy and the adjustment of the educational and training system offerings.

The best examples

Nothing proves better in addressing this challenge as cybersecurity education hubs and cybersecurity centres of excellences. Lately, there is no better example of this type of initiative than Advanced Technology Park on the campus of Ben-Gurion University in Beer Sheva in Israel. Which even aspires for the title of the New Silicon Valley - place, where technologies are mainly developed just in the field of cybersecurity. We introduce something that can be called an economic anchor, which will change Beer Sheva into a national and international centre of cybernetics and cybersecurity – said in September 2013 Israeli Prime Minister Benjamin Netanyahu, opening the first stage of this investment.

[1] Working Paper: Digital Economy - Facts & Figures, European Commission, p. 3 [online] .http://ec.europa.eu/taxation_customs/resources/documents/taxation/gen_info/good_governance_matters/digital/2014-03-13_fact_figures.pdf (access: 10.12.2015).

[2] European Commission, [online] http://ec.europa.eu/digital-agenda/en/grand-coalition--digital-jobs#Article (access: 20.12.2015).

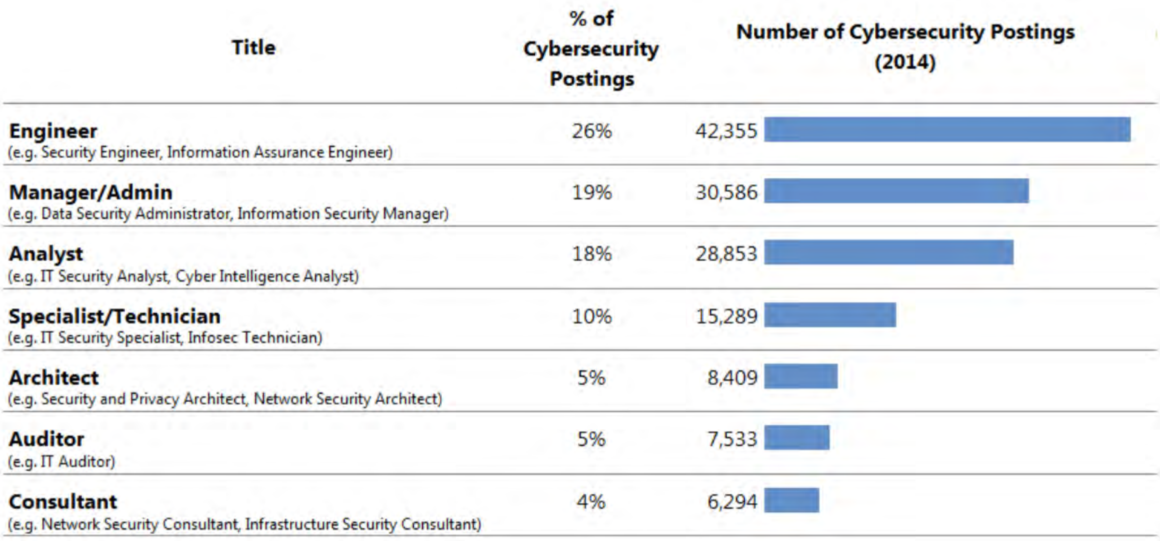
[3] Commission and EU ministers discuss digital skills and review of EU telecoms rules, [online] http://ec.europa.eu/digital-agenda/en/news/commission-and-eu-ministers-discuss--digital-skills-and-review-eu-telecoms-rules (access: 20.12.2015).

[4] Growing cyberthreat means more jobs in US, [online] http://www.cnbc.com/2015/08/06/growing-cyberthreat-means-more-jobs-in-us.html(access: 20.12.2015).

[5] 2014 Annual Security Report, [online] http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf (access: 20.12.2015).

[6] Job Market Intelligence: Cybersecurity Jobs, Burning Glass Technologies, 2015, p. 3 [online] http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf (access: 10.12.2015).

Table 3. The Cybersecurity Workforce Overview



Title	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)
Engineer (e.g. Security Engineer, Information Assurance Engineer)	26%	42,355
Manager/Admin (e.g. Data Security Administrator, Information Security Manager)	19%	30,586
Analyst (e.g. IT Security Analyst, Cyber Intelligence Analyst)	18%	28,853
Specialist/Technician (e.g. IT Security Specialist, Infosec Technician)	10%	15,289
Architect (e.g. Security and Privacy Architect, Network Security Architect)	5%	8,409
Auditor (e.g. IT Auditor)	5%	7,533
Consultant (e.g. Network Security Consultant, Infrastructure Security Consultant)	4%	6,294

Source: Job Market Intelligence: Cybersecurity Jobs, Burning Glass Technologies

After two years, we can say: in essence – it is essentially changing. And a human capital in this venture is at least as equally important as it is in financial terms.

Cybersecurity – both within domestic and international dimensions - is one of the main priorities of the Obama administration's security policy. In practice, it is also reflected in the adaptation of education system to address the sector's needs, developed together with close co-operation of commercial enterprises, government agencies (such as the National Security Agency, the Department of Homeland Security and the National Science Foundation) and universities.

In recent years, the US created numerous education hubs, regional centres of excellence specialising in cybersecurity, and national centres, such as the National Initiative for Cybersecurity Education at the National Institute for Standards and Technology. A strategy for workforce development has been established for the cybersecurity sector (National Cybersecurity Workforce Framework). A special emphasis is placed on the so-called STEM (which stands for Science, Technology, Engineering, Mathematics) in education. All of this together adds up to the national strategy of win-win, whereby particular cities and states are becoming important centres in the field of cyberspace education. As a result of the development in information technology, many academic centres are gaining significant comparative advantages in attracting investments of the cybersecurity industry.

Since 2011 the United Kingdom government within the National Cyber Security Programme has invested in establishing training providers and a network cyber education specialists. According "Strategic Defense and Security Review" [7] outlining the national defence strategy for the next five years, UK will speed this process up, providing targeted training for cybersecurity specialists. The schools programme to identify and encourage talent among 14–17-year-olds will be created across the UK, as well as new cybersecurity apprenticeships focused on particular sectors will be granted. UK is going to scale up existing successful programmes, including the Cyber Security Challenge and GCHQ's 'Cyber First' undergraduate sponsorship scheme. Another £20 million will be allocated to launch a new Institute Coding, which aim is to develop digital and computer science skills. Across the county in leading UK universities Centres of Excellences in Cyber Security Research have being established. The UK is also

7 | Strategic Defense and Security Review, p. 79 [online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (access: 18.12.2015).

encouraging young people to study engineering and science. All this initiatives are providing the UK with professionals with the right cyber skills for public and private sectors. Education is perceived by the UK government as a requirement to remain a world leader in cybersecurity.

We are not prepared yet

Most of the European countries are not systemically prepared to face cyberthreats and challenges, and its education systems have not kept pace with the market needs. This state of affairs threatens the internal, international and economic security. European decision-makers need to be aware of these threats and need to increase expenditures on education, and also solutions aimed at adjusting educational offerings should be adopted to be able to tackle challenges and to provide cybersecurity of the state, public institutions and business. It is essential to support the academic centres which serve as recruitment base for the broadly cybersecurity sector. This sector should become one of the priority areas research, as it has been announced by the European Commission on December 18th, at the beginning of the public consultations on the areas of work the future cybersecurity contractual public-private partnership. The Commission stated that "the PPP will be a contractual arrangement between the Commission and an industrial grouping, both of which are committed to supporting, in the EU's Horizon 2020 programme, research and innovation activities of strategic importance to the Union's competitiveness in the field of cybersecurity. A PPP bringing together industrial and public resources would focus on innovation following a jointly-agreed strategic research and innovation roadmap. It would make the best possible use of available funds through better coordination with member states and a narrower focus on a small number of technical priorities. It should leverage funding from Horizon 2020 to deliver both technological innovation and societal benefits for users of technologies (citizens, SMEs, critical infrastructure), as well as provide visibility to European R&I excellence in cyber security and digital privacy."[8]

> " Most of the European countries are not systemically prepared to face cyberthreats and challenges, and its education systems have not kept pace with the market needs.

A chance (not only) for Poland

According to European Commission, there is a room for improvement in terms of educating and employing ICT specialists in Poland. "With regard to the share ICT specialists as a percentage of employed individuals Poland ranks only 21st of all EU Member States. Even though Poland has more STEM (science, technology and mathematics) graduates than most countries in Europe, it does not yet manage to use this advantage in order to increase its share of ICT specialists."[9] For years, Poland has been famous for its information technology talents. Nothing is missing in the quality of academic centres, which have the potential to create cybersecurity related education offerings (including Warsaw, Wroclaw and Krakow). As the analysis of the Polish Information and Foreign Investment Agency shows, these cities have a variety of educational offerings providing a large number of young, well-educated computer scientists, programmers, network administrators, system analysts, security system engineers etc. These are particularly attractive places for IT industry investment. The cybersecurity sector is a "knowledge-absorbing" sector, further characterised by good dynamics of development and innovation, therefore it is a good investment for the future.

Thus, the regions which will support academic institutions in the development of computer science, especially related to the topic of cybersecurity, can become major national centres of education: "our Silicon Valleys" – supporting the security building measurements within the Polish cyberspace. Issues related to

[8] | Public consultation on the public-private partnership on cybersecurity and possible accompanying measures, [online] http://ec.europa.eu/digital-agenda/en/news/consultation-public-private-partnership-cybersecurity (access: 18.12.2015).

[9] | European Commission, Poland, [online] https://ec.europa.eu/digital-agenda/en/scoreboard/poland (access: 20.12.2015).

cybersecurity should not be restricted to strictly technical dimensions and to information technology because what happens in cyberspace increasingly makes an impact on public policies and legislation and it is an area of conflict and a matter of international relations. It is essential to upgrade the education offerings with a "cyber" component, such as political science, international relations, national security studies, public administration and law (both on master's and postgraduate level). Of course, the above-mentioned areas are not exclusive, but merely identify the most current needs.

Due to its competitive advantages, the most serious candidate for the city that could become a regional centre of education in Poland and in Central Eastern Europe, within the area of cybersecurity is Kraków. Today, the biggest Polish and global IT companies (such as Comarch, Cisco, IBM, Samsung) invest in this city as well as in the entire Malopolska Region, and also the largest number of start-ups related to technology is being created. In addition, the outsourcing industry employs huge number of employees (about 40 thousand) who are extremely vulnerable to cyberthreats. In the near future, further development in the Małopolska province may be also conditional upon the accessibility to network security specialists.

Krakow is currently the second academic centre in Poland, in terms of number of graduates in information technology (very slightly inferior to Warsaw). The city is also a hub of academic disciplines as humanities, within which experts and professionals can be trained and educated, and whose knowledge and skills can be utilised to build a solid foundation for the country's cybersecurity.

In Kraków, the biggest annual public conference in this part of the continent - the European Cybersecurity Forum - CYBERSEC was held, co-organised by the City of Kraków. This annual conference brings together specialists in this field and is a place to develop practical measures which are aimed at increasing cybersecurity within the Member States of the EU and NATO. It is a platform for community building, both for Polish and international experts, academics and professionals specialising in cybersecurity (understood as a challenge for state institutions, international organisations, business and military as well).

All of this potential can be used to create National Digital Staff Resources and contribute to the country's security growth and to the development of the city itself. It is also in the interest of not only the local authorities, but also of companies from the IT sector which are investing in the Małopolska province to stimulate universities in Krakow to educate more experts in the field of cybersecurity and to create a new "cyber-specialisation," thereby extending the scope of the educational offer. It is also important for the universities to realise that there is a real demand in the business and other sectors for "cybertalents." A push from the youth can be an important factor in this process – students should be aware that there is a "cybernetic employment gap" and by filling it, it provides career perspectives and guarantees a higher remuneration. This creates also a possibility to work in the field of national and/or economic security of the state. In this sense, it can be seen attractive for the youth, not only for financial reasons. This process requires the identification of all stakeholders, the creation of a platform for co-operation between them and the implementation of solutions which are strengthening this co-operation.

“ One of the most important challenges for the new government, including the Ministries of Digitisation, (...), is to provide a personnel with valuable skills and knowledge for our increasingly innovative and digital economy.

One of the most important challenges for the new government, including the Ministries of Digitisation, Science, Higher Education and Development in particular, is to provide a personnel with valuable skills and knowledge for our increasingly innovative and digital economy. Shifting the centre of gravity in the educational system of modern human resources in Poland has to, however, take place not only in just one city (Krakow), but also in the entire country. In the following years, we need to build together a competent "cybernation." ■