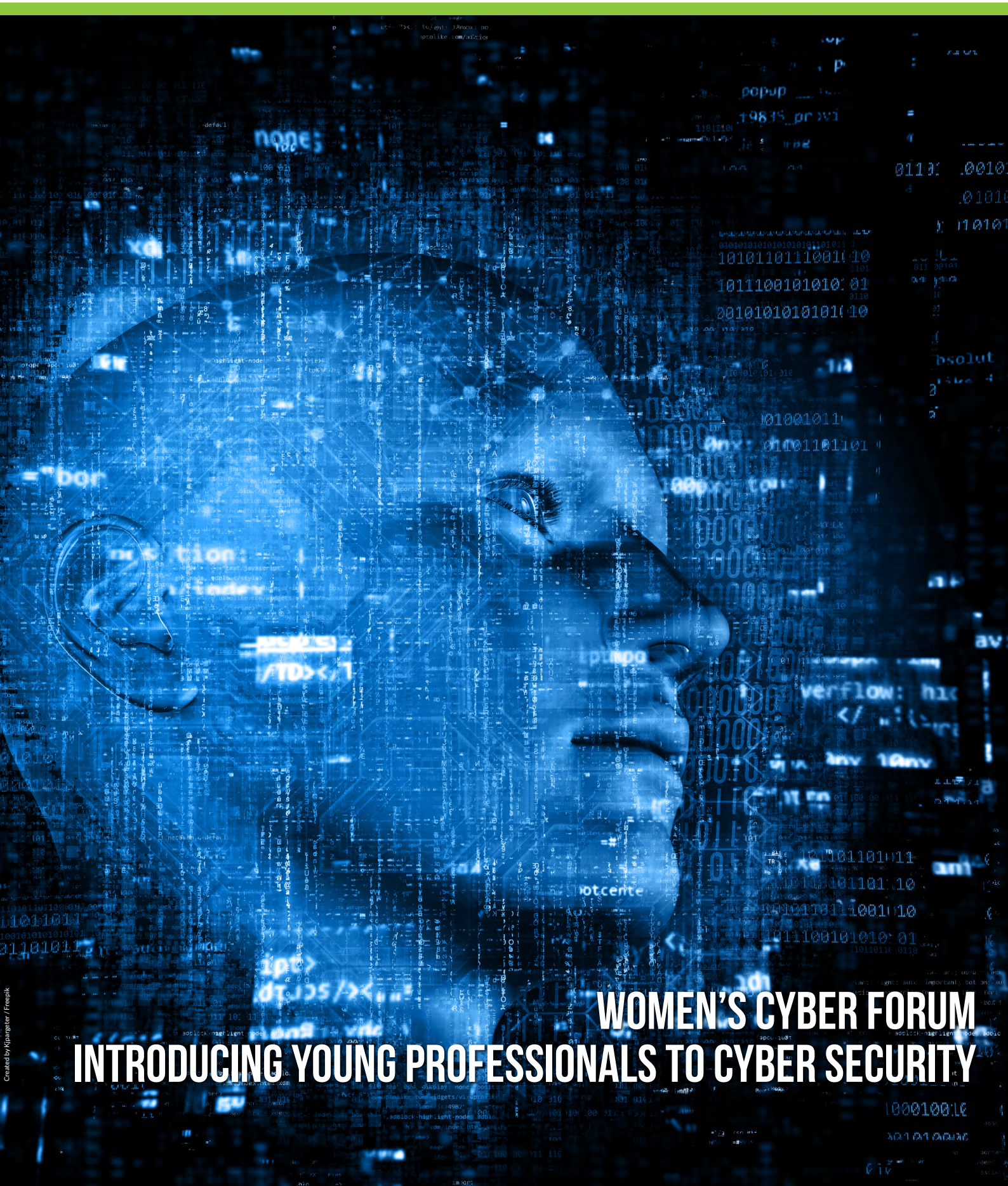
NEWSLETTER

Vienna, September 2017

energypact foundation



Created by Kjpargeter / Freepik

WOMEN'S CYBER FORUM

INTRODUCING YOUNG PROFESSIONALS TO CYBER SECURITY

energypact

WOMEN'S CYBER FORUM 2017

Launching Careers In Cyber Space

Information sharing - Networking - Mentoring

November 6, 2017
Vienna

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

REGISTRATION IS NOW OPEN

With the support of

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

More information available on: www.energypact.org/womencyberforum

EDITORIAL

The Energypact Foundation was established with a vision of fostering an international collaborative community of technologically and risk informed stakeholders for address today's needs and tomorrow's challenges of the energy sector. One of these challenges includes addressing cyber security including the need for developing and sustaining a cyber capable work force.

The Women's Cyber Forum is part of this effort. The idea for the one day event started out as a crazy discussion over coffee, but ended up being not so crazy after all and interest has just soared. The most challenging aspect of developing the programme has been coming up with a name for the forum.

Designed for young professional women (and men) with an interest in cyber security issues, the goal of this seminar is to create a forum for information sharing, networking and mentoring: to raise awareness and excitement about cyber security as a possible career choice. Often times, the term "cyber security" brings apprehension as it is seen as an enormously complex and technical field reachable by only a few.

We all have an inner geek – we must, as we are all users of computers and computer-based services. Our goal with this newsletter and the Forum is to foster interest, excitement, and conversation about cyber security. We may not all end up being cyber security experts, but it should be our goal to be cyber aware experts no matter what our chosen profession is.

This month's newsletter relates the experiences of and motivations of the organizational team for the Women's Cyber Forum.

Enjoy reading!

WOMEN'S CYBER FORUM TO INTRODUCE YOUNG PROFESSIONALS TO CYBER SECURITY

Andrew Bramnik, Emergency Response Training Officer, Department of Nuclear Safety and Security, International Atomic Energy Agency (IAEA)

Thousands of high-paying jobs are vacant and waiting for you; jobs in both the public and private sectors that offer the chance to make a difference, protect people locally and internationally, and get well-paid to do it.

Propose the following to a university student or young working professional and they will likely say that it's ***"too good to be true"***: Thousands of high-paying jobs are vacant and waiting for you; jobs in both the public and private sectors that offer the chance to make a difference, protect people locally and internationally, and get well-paid to do it. Some might think it's a scam. Others would claim that it's only for engineers or scientists with specialized PhDs. But they would be wrong.

Demand for cyber security professionals is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million according to Forbes Magazine.[1] As much as this critical field needs trained and dedicated workers, it desperately needs help from women: According to the 2017 Biennial Women in Cybersecurity Report, women comprise only 11 percent of the global information security workforce, even though on average women have higher levels of education than men and their more varied educational backgrounds contribute to a more diverse set of skills they can bring to the industry.[2]

The first-ever Women's Cyber Forum: Launching Careers in Cyber Space aims to correct that trend by introducing women and young professionals to opportunities in cyber security. The one-day seminar will feature presentations and networking opportunities from experts at private companies and government agencies. The event promises to be an engaging opportunity for university students and professionals in the first few years of their careers to meet experts from major companies in the field of cyber security.

The seminar is designed for young professional women (and men) with an interest in cyber security issues. Desired attendees include women and male allies already engaged or considering careers in cyber security, including university students and faculty, industry professionals, members of the government and professional organizations.

"It's important to me to conduct the Women's Cyber Forum because you need to be active to make a change," says Alessia Durczok, the Conference Scientific Secretary. "If you want to make a change for women then be active, be the chance." The Forum, organized by the Energypact Foundation, will not merely focus on cyber security from a technical perspective. Instead, attendees will hear about and participate in topics ranging from the Cyber Environment and Cyber Security Research to the Cyber Career Path and Building a Cyber Skill Set. ***"If you are interested but you do not know how to get involved, come to the Women's Cyber Forum and we will support you,"*** Durczok continues, ***"We want to empower attendees with the necessary tools and ideas to enter a vital field that is currently lacking a strong female component."***

The Energypact Foundation Women's Cyber Forum is being hosted by Diplomatische Akademie Wien on November 6, 2017. For more information and registration details, visit the conference website at https://www.energypact.org/womencyberforum/ or contact the organizers by e-mail at womencyberforum@energypact.org.

[1] https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#2bf3bf7227ea
[2] https://iamcybersafe.org/news_women_cybersecurity/

ALL WELCOME ON THE PATH TO CYBER: WOMEN AND UNCONVENTIONAL ROUTES TO CAREERS IN CYBER SECURITY

Colleen Glenn, Idaho National Laboratory, USA

The challenge remains to motivate more women to intrinsically contemplate education and jobs in cyber security as interesting, rewarding, and attainable rather than coming to the field by chance.

As so many aspects of life have become digitalized, the field of cyber security has necessarily grown in terms of technology, education, and career opportunities. With the continuous evolution of information technology (IT), comes an increasing need for experts to understand, mitigate, and prevent cyber threats.

Yet studies indicate that while cyber threats are growing exponentially in numbers and severity, the number of people considering a career in cyber is stagnant, with an anticipated shortage of 1.8 million cyber security professionals by 2022. Despite this impending shortfall, one group noticeably absent from the current number of cyber security professionals is women. Per the 2017 Global Information Security Workforce Study, women comprise only 11% of the information security workforce, a relatively small portion compared to women making up nearly half the total workforces of the U.S. and Europe. In order to encourage more women to fill the fast-increasing number of jobs in cyber security, it may be helpful to consider key factors that discourage female students and professionals from pursuing careers in cyber.

A commonly perceived setback may be that jobs in cyber security require technical experience or a science, technology, engineering and mathematics (STEM) background. However, cyber security needs perspectives from many kinds of professionals, often beyond what engineering or computer science experts can offer.

Though women (particularly among millennials) are increasingly represented in disciplines such as computer science and engineering, current number trends of female STEM-focused undergraduates are dwarfed by the projected need for cyber security professionals over the next decade. While the cyber security field needs STEM backgrounds and technical experience, it also requires the views of professionals from areas unconventionally associated with cyber to handle other aspects of cyber businesses including but not limited to management, analysis, and design. Cyber security professionals point out that in some technical aspects of cyber security design, those with roots in social science often offer much needed feedback in social engineering, user experience, and human error issues. Some tech-enabled businesses intentionally bring in non-technical staff from other departments provide ***"outsight"*** to engineers and developers. Some female cyber security professionals from non-STEM backgrounds found their way in cyber somewhat by accident: a former law expert's curiosity was mentored into a position as Vice President Digital Forensics, or an information governance manager at a gas company is intrigued by the possibilities a degree in cyber security might bring to her work. But, the challenge remains to motivate more women to intrinsically contemplate

education and jobs in cyber security as interesting, rewarding, and attainable rather than coming to the field by chance.

For those who are thinking about starting or rerouting to a career in cyber security or simply want to learn more about cyber-related techniques and issues, there are a number of free and easily accessible resources available including online college and certification-level courses, interactive programming applications, and e-communities and forums that provide discussion and networking opportunities, particularly for women interested in cyber.

For those considering transitioning into cyber security careers, tech literacy is important and can be improved by taking advantage of such resources. Proficiency in relative technology can help prospective cyber professionals have meaningful conversations with and gain the respect of tech experts such as engineers and programmers.

For cyber professionals and consumers alike, it is important to acknowledge that cyber security is also a personal responsibility in everyday life-knowledge of basic cyber hygiene for home and work computing is a fundamental first step to a cyber career path.

To address the anticipated shortage of cyber security professionals, employers have a responsibility to attract a more diverse workforce and to consider more qualified applicants from nontraditional backgrounds. The majority of the current cyber security workforce, (87% globally), come from unconventional or non-technical fields such as business, marketing, or military. The low numbers of women working or seeking careers in cyber security could be elevated by new

recruitment practices seeking to increase diversity and attract professionals from backgrounds other than those traditionally associated with STEM.

Further, cyber security business leadership can benefit from the growing number of female MBA graduates, though a recent Catalyst study indicates that only 18% of new female MBAs take managerial jobs at tech companies compared to 24% of men. The study also finds that the primary barriers to women in tech leadership are feeling like an outsider, unclear evaluation criteria, and a lack of role models. To gain better direction and more innovation, the cyber security industry must actively seek gender and experiential diversity, and foster an environment that encourages more female mentorship. This kind of change in cyber security culture could contribute to fewer threats to and greater security for our digital lives.

[3] https://iamcybersafe.org/research_millennials/

[4] 2017 Global Information Security Workforce Study: Women in Cyber security (https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf)

[5] "In many countries, at least four-in-ten in the labor force are women" (http://www.pewresearch.org/fact-tank/2017/03/07/in-many-countries-at-least-four-in-ten-in-the-labor-force-are-women/)

[6] 2017 Global Information Security Workforce Study: Women in Cyber security (https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf)

[7] "Women in Information Security: Emily Crose" https://hackernoon.com/women-in-information-security-emily-crose-5eddad84f065

[8] "The 11%; where are the women in cyber-security?" (https://www.scmagazineuk.com/the-11-where-are-the-women-in-cyber-security/article/579303/)

[9] "Women in Tech: Breaking the Digital Ceiling" (https://www.alumni.hbs.edu/stories/Pages/story-bulletin.aspx?num=4494&utm_campaign=Socialflow&utm_source=Socialflow&utm_medium=Tweet)

GREAT MINDS DON'T THINK ALIKE AND HOW THE MOTH BECAME A BUG

Alessia Durczok, Women's Cyber Forum Scientific Co-Secretary

Here is a conversation that I had a few years ago. ***"Do you own a computer"***, my Cyber Security colleague asks me? ***"Yes, I do". "And do you have a cell phone?" "Yes, I do." "And what do you know about Cyber Security? "*** There is a chronic underrepresentation of women in cyber security. However, it is a topic that we encounter every single day in our lives. Why should women not be part of it? Don't you do online banking, for instance? Start digging the internet and you will find that there were great female thinkers throughout time, who left their traces in the Cyber space. Let me introduce you to a few of them.

Ada King, the Countess of Lovelace (1815-1852)

When you are talking about the origins of programming, people often think of Ada Lovelace. Her ability to combine spatial sense and mathematics sparked her idea to create a machine that would write music or create graphics. During her time, society assumed the ability for logical thinking in the male brain. It was a preconception that created barriers in people minds, leading to specific roles genders would have to fulfil. Ahead of her time and society, she unfortunately, never saw her vision come true. Nevertheless, she remains a role model for women today.

The many women programmers of ENIAC

Fast forward a hundred years. The role of women in society had changed since the Countess of Lovelace and women were finally admitted to university programmes. As horrible as World War II was, it created an opportunity for women to enter scientific jobs. It was a time, when trained mathematicians were badly needed in the US military, in order to calculate ballistic missile routes. Men and women who studied mathematics were hired and very soon the military counted six distinguished women as part of their team which was working on one of their biggest data-processing projects, entitled the Electronic Numerical Integrator and Computer - or short ENIAC. Kay McNulty, Betty Jennings, Betty Snyder, Marlyn Meltzer, Fran Bilas, and Ruth Lichterman were the first programmers of ENIAC, though it took many years until their work was recognized.

Grace Murray Hopper (1096 – 1992) and her famous moth

Excited by the first computers, Grace Hopper had the early vision that computers could be applied in many different fields. She understood that it had to become easier for anyone to use these machines. She pioneered the beginnings of software and on the way coined software language which is still relevant today. While working at a Mark II Computer, her colleagues found a moth stuck in a relay. It had stopped the proper functioning of the computer. The moth was removed and glued into the logbooks of the project. The terms 'bug' or 'debugging' had been used in the engineering field long before the incident, but has ever since then marked a special moment in the history of computers.

These were just a few female role models of many in Cyber Space. It is essential to discover the diversity of their thinking and achievements for technology during different times in history. Even more importantly, one must recognise the foundations which they created in their times, influencing technology, society and history.

Today, the traditional role model-thinking is challenged. We have come a long way since Ada Lovelace but there is still a long path ahead of us. The future of Information technologies will be shaped by science but also by politics, economics and societal changes. IT touches almost every aspect in life. Though, women are not represented in every aspect of IT. Women must demand and claim their places. Great minds do not think alike. They all think differently no matter if they are male or female. Including the female perspective in technology will not only enrich technology but also carry forward the change in society. Let's close the growing gender gap in tech!

RESEARCH CHALLENGES IN CYBER SECURITY

Maria Leitner, Center for Digital Safety & Security,
Austrian Institute of Technology (AIT)

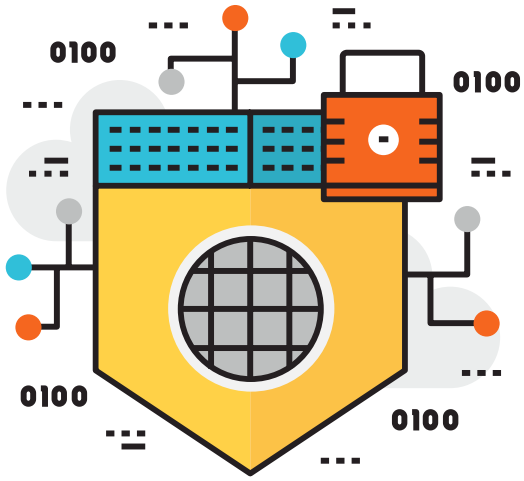
Today's modern society is facing the digitalization of our world. Billions of people are connected with devices, relying on their functionality, security and permanent availability. For example, 8.4 billion connected "things" on the Internet of things will be in use in 2017 that will be utilized in businesses (such as in Industry 4.0, healthcare, smart buildings) or consumer segments (e.g. smart homes, smart meters).

For example, OECD expects that the new production revolution will use interconnected technologies to enable new processes in industrial production which can lead to new products and services. Securing these digital technologies will be one of the major challenges in the forthcoming decade.

Research engages in multiple facets to develop methods and tools in cyber security and contribute to international cyber security standards. Measures can be developed for various application areas such as cyber-physical systems, autonomous driving, smart homes and healthcare. Ideally, system development for all these application domains starts with developing a safe and secure design. Preventive security measures are essential when it comes to building secure systems. Additionally, it is important to understand interconnections and connected systems, which interact and communicate among each other, and how they can affect each other in case of attacks. Furthermore, research contributes to test and verify existing technologies to further enhance security and to avoid vulnerabilities or errors.

Another important aspect is the detection and management of (information security) incidents, i.e. an unplanned event that could compromise the security of information or weaken or impair business operations, after an incident has occurred. This includes e.g., identifying, analyzing and mitigating incidents as well as preventing reoccurrence (e.g., with computer security incident response (CSIRT) teams). Incident management is often concerned at organizational level but can become a matter of national security. That's why information sharing and exchange has become a key factor to enable faster incident response times and increase the effectiveness of mitigation activities to resolve and analyze incidents.

Cyber security does not only relate technologies – it depends on how humans conduct their daily business. For example, cyber security affects all: from the general staff being aware of phishing mails, accountants being aware of CEO fraud campaigns to CSIRT experts that mitigate incidents. Trainings and exercises can support to maintain awareness and increase competencies of participants. Virtual training facilities such as cyber ranges can offer individual training scenarios for awareness are trained, processes for incident management are improved or information sharing of threat intelligence can be tested.



[10] 2017 Global Information Security Workforce Study (https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf)
[11] The Gender Divide in Tech-Intensive Industries (http://www.catalyst.org/knowledge/gender-divide-tech-intensive-industries)
[12] Gartner (2017), Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, February 7, 2017, http://www.gartner.com/newsroom/id/3598917.
[13] OECD (2017), The Next Production Revolution: Implications for Governments and Business, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264271036-en

MAINSTREAMING CYBER SECURITY

Andrea Cavina, Director for Training and Education Development, Energypact Foundation

Civilization is rapidly advancing towards a time when having an adequate understanding of cyber security will grow to embody a societal and personal value comparable to what currently is represented by understanding road safety and/or having a driving licence (while at the same time this latter skill may wane as autonomous vehicles will render it obsolete). We witness a continuous migration towards networked digital systems of large chunks of core societal functions, key information, and human-human interactions. This trend is rapid, unstoppable and to a large extent desirable but it implies that we, as individuals and as a society, will be exposing near 100% of our vital capabilities and functions to the possibility of digital compromise.

As the only possible answer to such unprecedented exposure, cyber security has to become a pervasive skill that is absorbed progressively and continuously. In a way not dissimilar to how teaching children to cross a road or to cycle to school alone for the first time are some of the obvious steps in the safe education of future citizens, so have we to understand and implement cyber security as a basic building block of our society. The urgency lies in the fact that this change has to start from now and has to rapidly encompass the population as a whole.

Moving towards the integration of cyber security into the very fabric of what we understand as safe, secure, competent and responsible civic behaviour requires a vast multi-dimensional leap in effort, reach, awareness, and the ability to make existing knowledge available and serviceable. We surely recognize the enormous effort that the security industry and the academic community are investing into constantly developing new tools and methodologies. These cover a broadband spectrum and are aimed at anything from securing systems used by the widest public to tackling new attacks or protecting niche systems that may have been out of the radar of attackers just a few years ago.

Nevertheless, there is a huge risk associated in the magical – and yet too common – belief that technology alone can solve problems that have economical, psychological, anthropological and legal facets and that are associated to some of the most radical shifts in societal attitudes and habits witnessed in the last centuries.

The common effort towards cyber security, to be successful and sustainable, has to become global in scope and in reach. It has to extend their grasp beyond specialized agencies and niche industries to involve – and not as simple sidekicks! – all those aspects of security that complement or transcend technology and can affect and change the approach that we have to defending our digital assets. The security workforce not only has to grow in strength and competence but also to diversify itself to ensure that solid competences and a thorough understanding of crucial issues are available in all sectors and to all practitioners.

It's in this view that the current unjustified balance in the gender composition of the security workforce stands out as a preferred target. Besides the necessary but effectively longer-term goal to increase women's participation in STEM fields, there are crucial untapped resources in fields where parity has long been reached if not surpassed which could be easily converted and integrated in a wider and more holistic security configuration. Lawyers, legislators, regulators, psychologists, educators, just to name a few, are crucial to an organic expansion of the role cyber security should have in our society. Providing additional training to practitioners in these fields to refocus their skills around cyber can be a key investment both for gender parity and for a safer and sounder society.

The halo of mystery and of inaccessibility that the field shows to the world has to be demystified and deconstructed and a conscious effort has to be made to visibly open new pathways, new careers, new roles not just at the periphery of cyber but at its very core. Only in this way can we hope, as a global society, to educate ourselves and to prepare for the challenges that are already mounting above the horizon.

[14] See ISO 27000 definitions

[15] T. Pahi, M. Leitner, und F. Skopik, "Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers", 3rd International Conference on Information Systems Security and Privacy, 2017, p. 334–345.

CYBER SECURITY, THE LAWYERS AND THE LAW

Paulina Giżowska,
Department of Nuclear Safety and Security, IAEA


Designed by awesomecontent / Freepik

Lawyers are not the first thing that comes to mind when you think about cyber security and possible careers. You tend to think an IT or computer background is a prerequisite to even start thinking about cyber security. You might even think of cyber as a whole different scary underground world hidden in the meanders of the World Wide Web. However, lawyers in cyber security are on the up and up and they are here to stay.

There is no international management of cyberspace and no proper global governance. As of yet, there is not even an international cyber law. Mutual distrust between the main cyber superpowers allows limited cooperation and even less so when it comes to finding a common approach to regulating the cyber world. Due to the relative novelty of the topic and the persisting mistrust between States with the largest cyber capabilities, there is little international understanding about what constitutes a cyber aggression, how to attribute it and how to respond. At the same time, legal cyber literature is now flourishing.

The law of cyber security is an emerging field of law, providing an exceptional opportunity for international lawyers to contribute to something new. Until now, international lawyers were mostly preoccupied with finding innovative approaches to centuries' old problems: statehood, law of treaties, State responsibility for internationally wrongful acts, use of force, law of armed conflict, etc. Lawyers are thus grasping this unique opportunity to position themselves as revered scholars in a new field – something they can hardly do in other areas of international law, long since established. The legal challenges requiring research and study are numerous.

How far can the current international framework be stretched to include cyber security? Should a completely new set of rules be established and how to do so? Law making on an international level is not straightforward.
Also, on the domestic level cyber lawyers are in high demand. Law firms are increasingly turning to this new practice area, establishing consulting services in the field. Increasingly, even law firms not practicing in cyber need some cyber protection as they may be vulnerable to cyber-attacks: their work and reputation depends upon protecting sensitive data and maintaining clients' confidentiality.

The cyber lawyer cannot only be a lawyer: she or he has to understand technology and threats, be able to grasp the main concepts. While you do not have to be a computer or IT expert, having some technical knowledge helps. Cyber law is a mix of technical and legal issues, and this mix makes it a fascinating field to practice.

Today's nuclear world is also a cyber world: it is a dynamic world with rapidly evolving technologies, which has to face changing threats coming from increasingly imaginative malicious actors using increasingly sophisticated methods. Strategies must be constantly evaluated and updated so as to effectively address current and emerging threats. The approach to securing cyberspace has to be multi-disciplinary in order to be always ahead of the game. Lawyers can help build a framework for that.

Designed by Jannoon028 / Freepik

[16] For a comprehensive analysis of how existing international law applies to cyberspace, see: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press (2017)
[17] For a counterargument and extensive research into legal 'interventionism', see J. d'Aspremont, Cyber Operations and International Law: and Interventionist Legal Thought, 21 Journal of Conflict and Security Law (2016). Available at SSRN: https://ssrn.com/abstract=2765408
[18] For more on this topic, see: "What is cybersecurity law and what do cybersecurity lawyers do" at https://www.rsaconference.com/blogs/what-is-cybersecurity-law-and-what-do-cybersecurity-lawyers-do

CYBER SECURITY NEWS DIGEST AUGUST 2017

CYBERSECURITY: AN OPEN PLAYING FIELD FOR WOMEN

Last year, Forbes reported nearly one million global cyber security jobs were left unfilled, with demand expected to grow to six million by 2020. In this period, the cyber security market is expected to rise to $170 billion in worth. Only about 10 percent of all cyber security positions globally are filled by women, according to Rowe. Many organizations, including BYU's Cyber security Research Lab, work to encourage women to take advantage of these open jobs, which often benefit from an increase in diversity.

More info: http://universe.byu.edu/2017/08/31/cybersecurity-an-open-playing-field-for-women1

WOMEN IN CYBER SECURITY FACE PERSISTENT BARRIERS, RESEARCH REVIEW CONFIRMS

Women in cyber security face "persistent and enduring barriers" a review of research commissioned by the Office of the Cyber Security Special Adviser has revealed. The review, published yesterday and carried out by UNSW Canberra Public Service Research Group and UNSW's Australian Centre for Cyber Security, examined existing academic and industry literature on female participation in the cyber security industry and related roles.

More info: https://www.computerworld.com.au/article/626363/women-cyber-security-face-persistent-barriers-research-review-confirms

CYBER PROGRAM TO SIGN UP WOMEN

The Office of the Cyber Security Special Adviser in the Department of the Prime Minister and Cabinet (Australia) is to host a mentoring program for women as part of its response to research revealing a shortage of female representation in the cyber security industry. According to the Department the research, Women in Cyber Security Literature Review, found that women comprised 11 per cent of the cyber security workforce globally, and just 10 per cent in the Asia-Pacific. "As the worldwide gap between qualified security professionals and unfilled positions climbs towards a projected 1.8 million by 2022, attracting and retaining women in cyber security professions is a crucial part of ensuring Australia's cyber resilience," it said.

More info: http://www.psnews.com.au/aps/566/news/cyber-program-to-sign-up-women

TECHNET PANEL DISCUSSES LACK OF WOMEN IN CYBER SECURITY INDUSTRY

Thousands of people are in downtown Augusta for TechNet, a cyber security conference for the military, defense contractors and civilians. Dozens of private companies packed in the Augusta Convention Center. All of them brought new cyber-security software and equipment for the military.

More info: http://wjbf.com/2017/08/09/technet-panel-discusses-lack-of-women-in-cyber-security-industry

FOR COLLEGE STUDENTS, CYBER SECURITY A MUST

As they head off to college, many students are alone for the first time in their lives, left to forge their own way through some of life's biggest challenges. The authorities are warning students to make sure their computer and mobile devices are protected. The most effective way to do that, they say, is to purchase security software and keep it up to date.

More info: http://www.thesunchronicle.com/news/local_news/for-college-students-cyber-security-a-must/article_6cfb27cd-424d-58a2-981d-1bf094043669.html

BUNDESKANZLERAMT ÖSTERREICH

EUROPE INTEGRATION FOREIGN AFFAIRS
FEDERAL MINISTRY
REPUBLIC OF AUSTRIA

FEDERAL MINISTRY OF DEFENCE AND SPORTS

BM.I REPUBLIC OF AUSTRIA
FEDERAL MINISTRY OF THE INTERIOR

bmvit
Federal Ministry
for Transport,
Innovation and Technology

energypact foundation

VIENNA CYBER SECURITY WEEK 2018

Protecting Critical Energy Infrastructure

Intergovernmental & Multistakeholder Conferences – Training – Technology Exhibition

CSP AUSTRIA

29 January - 02 February

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

SAVE THE DATE

With the support of

DIGITAL CITY WIEN

KURATORIUM SICHERES ÖSTERREICH

Should you have an interest in presenting or event sponsorship, please contact: viennaproject@energypact.org

energypact foundation

VISION

An international collaborative community of technologically and risk informed leadership, researchers, implementers, and stakeholders for the development, sustainability, and security of energy production, transmission, and delivery addressing today's challenges and tomorrow's needs.

MISSION

The Energypact Foundation has directed its efforts toward three mission areas:

AWARENESS:

Promoting dialogue and international co-operation on security issues for the energy sector.

TRAINING:

Establishing the Industrial Control Systems Security Centre (ICS Security Centre) in Vienna, Austria and regional training centres around the world for providing human resource development activities for leadership, management and employees.

RESEARCH:

Nurturing a collaborative research network for the energy sector.

energypact foundation

Become a Collaborating Member of the Vienna Project

Energypact Foundation
viennaproject@energypact.org
www.energypact.org