VOLUME 10, ISSUE 4, 2020

per Concordiam

Journal of European Security and Defense Issues

■ **ENERGIZING THE NETWORK**
A collaborative approach to training

■ **THE PORTUGUESE METHOD**
A human-centric focus on security development

■ **GERMANY'S CYBER RESERVES**
Building a formidable defense force

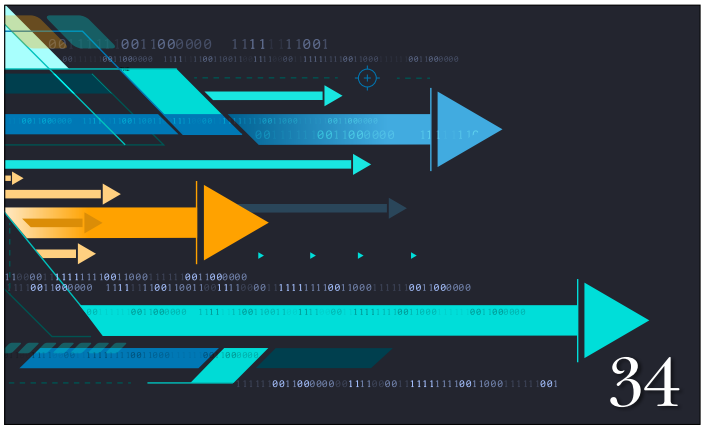
■ **SEEKING ANALYTICAL SUPERHEROES**
Assessing the nontechnical aspects of cyber threats

PLUS
Building a child online protection plan
Albania's security training and certification
Bridging the talent gap in the Philippines

THE URGENT NEED FOR

CYBER SECURITY WORKFORCE DEVELOPMENT

features



7 Cyber Workforce Development to Meet Today's National Defense Challenges

By Tom Wingfield, OSD(P)/HD&GS/DASD for Cyber Policy

10 Energizing A Workforce Ecosystem

By Danielle Santos, program manager, National Initiative for Cybersecurity Education at the National Institute of Standards and Technology, United States Department of Commerce

It takes partnerships and planning.

16 A Human-centric Approach

By Dr. Pedro Xavier Mendonça, Daniela Santos, Isabel Baptista and Lino Santos, Portuguese National Cybersecurity Centre

Portugal focuses on the individual.

20 Incentivizing Private Entities

By Atsuko Sekiguchi, deputy counselor, International Strategy Group, National center of Incident readiness and Strategy for Cybersecurity (NISC), and cabinet secretariat, government of Japan

How government procurement can boost cyber security.

24 At The Ready

By Rupert Brandmeier, Jörn-Alexander Heye, Dr. Florian Rupp and Clemens Woywod, military reserve officers, German Cyber and Information Domain Service

Advancing the German Cyber Reserve.

30 The Need for Analytical Superheroes

By Ondřej Rojčík, head of Strategic Information and Analysis, Czech National Cyber and Information Security Agency

Addressing the nontechnical aspects of cyber threats.

34 The Best Path Forward

By Pedro Janices, academic coordinator for the CAPA 8 Foundation; Mariana Galan, legal advisor to the Directorate of Cybercrime in the Ministry of Security of Argentina and member of the Commission on Public Policies, Human Rights and Digital Privacy for the CAPA 8 Foundation; Maximiliano Scarimbolo, principal officer for the Buenos Aires City Police; and Agustin Malpede, lawyer specializing in information law at the University of Buenos Aires

How to effectively develop a regional cyber security workforce.

40 A Collaborative Approach

By Jelica Vujadinović and Dr. Marko Krstić, Serbian National Computer Emergency Response Team

Serbia's cyber security education, training and workforce development strategy.

departments

44 Bridging the Talent Gap
By Genalyn B. Macalinao, information technology officer, Philippine Department of Information and Communications Technology
How the Philippines is coping with the overwhelming demand for cyber security professionals.

46 Defending Mauritius Against Cyber Threats
By Madan Kumar Moolhye, Information Technology Security Unit, Mauritius Ministry of Information Technology, Communication and Innovation
The nation's G-SIRT fights the never-ending battle to build cyber defense capacity.

50 Perfect Symbiosis
By Veronika Netolická and Petr Novotný, National Cyber and Information Security Agency of the Czech Republic
Cyber security exercises and national policies.

54 Building Albania's Cyber Cadre
By Dr. Vilma Tomco, director-general, and Klorenta Janushi, information security expert, National Authority for Electronic Certification and Cyber Security, Council of Ministers, Republic of Albania
A look at gaps in education, professional training and certification in cyber security.

58 Breaking the Triangle of Distrust
By Dr. Maximilian Schubert, secretary-general, Austrian Association of Internet Service Providers
Mutual respect and trust are prerequisites for mastering cyber security challenges.

62 Securing the Future
By Racky Seye, head of the Office of Information Systems Security and Digital Trust, Senegal Ministry of Digital Economy and Telecommunications
Child Online Protection Action Plan.

in every issue

4 DIRECTOR'S LETTER
5 CONTRIBUTORS
7 VIEWPOINT
66 CALENDAR

BOOK REVIEW

64 *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*
By Ben Buchanan
Reviewed by: Patrick Swan, *per Concordiam* contributor
As digital technology permits ever more precise delivery of conventional munitions, cyber technology remains often a mere blunt, uncontrollable, and uncalibrated area-wide instrument of power.

on the cover:

Finding, training and retaining skilled cyber workers is now essential to national security.

PER CONCORDIAM ILLUSTRATION

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Welcome to the 40th issue of *per Concordiam*. Scarcity of human talent is among the most pressing cyber security concerns for nations the world over. By one respected measure, the global workforce shortage is projected to exceed 1.8 million unfilled positions by 2022. Nations increasingly rely not just on robust cyber defense but on cyber security for commerce, education, health care and other key facets of modernity. Such reliance means that today's cyber security workforce gaps are tomorrow's national security challenges.

The United States has led the development of national guidelines for workforce development, expanding efforts from the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) to reach a broadening international partner network. In an era when government comes under sharp criticism, the NIST National Initiative for Cybersecurity Education (NICE) shines as an example of how government can convene and energize diverse transnational networks for positive change. The NICE framework was designed as an adaptable system for all elements of governmental and civil society to use in designing cyber security educational and workforce development strategies.

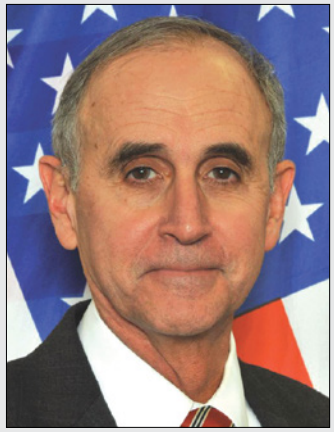
At its core, cyber security is a distributed challenge. By virtue of education and national priorities, some nations enjoy relative advantages while others may find the need to import talent as they grow their cyber security workforce from the bottom up. This issue of *per Concordiam* provides diverse examples of worldwide perspectives. As with other cyber security challenges, workforce development works best in partnership, with civil society, academia, private industry and governmental institutions working together. Looked at through the lens of government, private industry may offer what appears to be insurmountable challenges in the form of greater remuneration than what government can offer. With workforce development, government is learning that its competitive edge lies in its relative stability and in investments that can be made to retain talent. Training, long-term satisfaction, and meeting a national calling to service are just a few of the factors that government should prioritize to help surmount cyber security workforce challenges.

The Marshall Center's Program on Cyber Security Studies (PCSS) resident course enhances dialogue and learning on cyber workforce development in its many guises. In addition to cyber workforce development, the course includes related modules on cyber security strategy development, citizen awareness, whole-of-government solutions, certifications, standards and guidelines. The demand for more cyber-focused education grows each year. I encourage you to consider the recommendations of this issue's authors. You have a leading role to play by enhancing cyber security within your organizations and beyond. Take a step and take action!

We invite your comments and perspectives on this subject. Please contact us at editor@perconcordiam.org

Sincerely,

Keith W. Dayton
Director



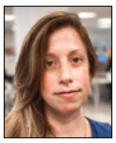
Keith W. Dayton

Director, George C. Marshall European Center for Security Studies

Keith W. Dayton retired as a Lieutenant General from the U.S. Army in late 2010 after more than 40 years of service. His last assignment on active duty was as U.S. Security Coordinator to Israel and the Palestinian Authority in Jerusalem. An artillery officer by training, he also has served as politico-military staff officer for the Army in Washington, D.C., and U.S. defense attaché in Russia. He worked as director of the Iraqi Survey Group for Operation Iraqi Freedom in Iraq. He earned a Senior Service College Fellowship to Harvard University and served as the Senior Army Fellow on the Council on Foreign Relations in New York. Gen. Dayton has a bachelor's degree in history from the College of William and Mary, a master's degree in history from Cambridge University and another in international relations from the University of Southern California.

Isabel Baptista is the Development and Innovation Department coordinator of the Portuguese National Cybersecurity Centre. She holds a master's degree in Information Security and Cyberspace Law, for which she developed a dissertation on the human factor in cyber security. For many years she was an IT trainer in public schools as well as in the private sector. In recent years, her main activities have been focused on raising awareness of the importance of cyber security by training citizens and organizations.

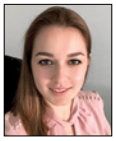
Rupert Brandmeier has held various managerial positions in the international business environment. He has extensive experience as an academic researcher and lecturer in the fields of business administration and economics, cyber security and archaeology.



Mariana Galan is a legal advisor in the Directorate of Cybercrime in the Ministry of Security of Argentina. She has previously been a technology legal advisor at the Cabinet Office of Ministers, the Ministry of Modernization and the Ministry of Foreign Affairs. Since 2016, she has served on the Commission on Public Policy, Human Rights and Digital Privacy of the CAPA 8 Foundation and is in charge of the cyber woman initiative.

Jörn-Alexander Heye is a German signal officer (reserve) with more than 28 years of experience, many of them in international missions in the United Arab Emirates and the Middle East. He has been a senior principal consultant, team leader, project manager and program manager in various technical and business projects in Germany and abroad.

Pedro Janices is the founder and the academic coordinator of the CAPA 8 Foundation. He is an advisor in the Department of Cybercrime Investigations in the Ministry of Security of Argentina. He served as national director of Critical Information Infrastructure Protection & Cybersecurity and national director of the National Office of Technologic Information, both in the Chief of Cabinet Ministers. Previously, he was director of technology and security at the Ministry of Justice, Security and Human Rights and director of technology and security at the Homeland Ministry.



Klorenta Janushi is an information security expert and works at the National Authority for Electronic Certification and Cyber Security at the Council of Ministers of Albania. She is a board member of Women in Technology in Albania and helped establish the Women4Cyber initiative, which was developed to increase women's participation in the cyber field.

Dr. Marko Krstić is senior security advisor in the Serbian National Computer Emergency Response Team. He specializes in machine learning solutions for cyber security. He is involved in several international projects on digital forensics evidence analysis via intelligent systems and practices; on transnational collaboration on bullying, migration and integration at schools; and the Next Generation Internet Trust initiative Project Casper.

Genalyn B. Macalinao is the policy lead of the Cybersecurity Bureau of the Philippine Department of Information and Communications Technology. She is one of the authors of *Towards a Resilient Regional Cyber Security: Perspectives and Challenges in Southeast Asia*, published in 2019, and was a lead contributor to the Philippines National Cybersecurity Plan 2022.

Agustin Malpede is a lawyer specializing in information law at the University of Buenos Aires in Argentina. He works as an advisor at the CAPA 8 Foundation and as a legal advisor within the Office of Undersecretary of Administrative Innovation.

Dr. Pedro Xavier Mendonça is a consultant at the Portuguese National Cybersecurity Centre, where he is the coordinator of the Cybersecurity Observatory and collaborates in the Awareness and Training Program, as well as a researcher and professor. His research focuses on social studies of technology, with an emphasis on the relationship between technological development and communication and users. His recent work examines the role of human behavior in cyber security.

per Concordiam

Journal of European Security and Defense Issues

Cyber Security Workforce Development

Volume 10, Issue 4, 2020

Contributing Editors
Philip Lark
Sean Costigan

George C. Marshall European Center for Security Studies

Leadership

Keith W. Dayton
Director

Dieter E. Bareihs
U.S. Deputy Director

Helmut Dotzler
German Deputy Director

Marshall Center

The George C. Marshall European Center for Security Studies is a German-American partnership founded in 1993. The center promotes dialogue and understanding between European, Eurasian, North American and other nations. The theme of its resident courses and outreach events: Most 21st century security challenges require international, interagency and interdisciplinary response and cooperation.

Contact Us:

per Concordiam editors
Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
editor@perconcordiam.org

per Concordiam is a professional journal published quarterly by the U.S. European Command and the George C. Marshall European Center for Security Studies that addresses defense and security issues in Europe and Eurasia for military and security practitioners and experts. Opinions expressed in this journal do not necessarily represent the policies or points of view of these institutions or of any other agency of the German or United States governments. Opinions expressed in articles written by contributors represent those of the author only. The secretary of defense determined that publication of this journal is necessary for conducting public business as required of the U.S. Department of Defense by law.

ISSN 2166-322X (print)
ISSN 2166-3238 (online)

Madan Kumar Moolhye is a cyber security professional at the IT Security Unit of the Ministry of Technology, Communication and Innovation of Mauritius. He has more than 14 years of experience in information and communications technology network operations and support management, and more than seven years of experience in project management and cyber security. He is a Certified Information Security Professional (2014) and a certified Lead Auditor (2006) for the ISO/IEC 27001 Information Security Standard.

Veronika Netolická is head of the National Strategy and Policy Unit at the Cyber Security Policies Department of the National Cyber and Information Security Agency of the Czech Republic. In 2018, she worked as a long-term researcher in Vietnam at the Ho Chi Minh University of Technology.

Petr Novotný is head of the Cyber Exercise Unit at the Cyber Security Policies Department of the Czech National Cyber and Information Security Agency. Among his responsibilities is the education of public sector employees through workshops and training sessions.

Dr. Ondřej Rojčík is the head and co-founder of the Strategic Information and Analysis Unit at the National Cyber and Information Security Agency of the Czech Republic. He has over 14 years of experience analyzing international security issues, including for the Czech Ministry of the Interior and for NATO. He holds a master's degree in security studies from University College London and a Ph.D. in international relations from Masaryk University in Brno, Czech Republic.

Dr. Florian Rupp has been involved in cyber and digitalization projects as director of the think tank Cyber & Innovation Labs, as chief digital officer of RailMaint GmbH, and as senior project manager and principal consultant at BWI GmbH. He is an associate at the Research Center for Cyber Defense at the University of the German Armed Forces and the Technische Universität München.

Daniela Santos is a doctoral student in public policy and is dedicated to the study of cyber security. She is a member of the Reflection Group on Cyber Resilience at the National Defence Institute. Since 2018, she has served as the Cybersecurity Awareness and Training project manager at the Portuguese National Cybersecurity Centre.

Danielle Santos is the program manager for the U.S. National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology, where she leads the administrative, organizational and communication functions of the NICE program office and its international outreach strategy. She has served as program manager for cyber security formal education programs, including at the National Centers of Academic Excellence and the CyberCorps and Scholarship for Service at the U.S. Department of Homeland Security.

Dr. Lino Santos is the head of the Portuguese National Cybersecurity Centre and an appointed member of the board of directors of the European Agency for Cybersecurity. He was previously the director for security and users' services at the National Foundation for Scientific Computing. He holds certifications in managing computer security incident response teams from Carnegie Mellon University and from the Marshall Center's Program on Cyber Security Studies.

Maximiliano Scarimbolo is a principal officer in the Buenos Aires City Police. He has worked for 22 years in the areas of prevention and investigation of complex crimes and protection of dignitaries. He is also part of the CAPA 8 Foundation. He works as a teacher of various professional law enforcement specializations.

Dr. Maximilian Schubert is the secretary-general of the Austrian Association of Internet Service Providers (ISPA). His main fields of expertise cover ISP liability law, telecommunication surveillance and law enforcement in the online sphere. He also serves as president of EuroISPA, the largest world-wide ISP association, where he is chairman of the Cybersecurity Committee.

Atsuko Sekiguchi is deputy counselor of the International Strategy Group, National center of Incident readiness and Strategy for Cybersecurity (NISC), cabinet secretariat in the government of Japan, where her responsibilities include coordinating national cyber security policy and forming international collaboration in cyberspace.

Racky Seye is an engineer in electronics and telecommunications who heads the Office of Information Systems Security and Digital Trust in the Information and Communications Technology Directorate of the Ministry of Digital Economy and Telecommunications of Senegal. She is a member of the Study Group 17 (Security) of the Bureau of Standardization of the International Telecommunication Union. She also participates in the work of the Global Forum on Cyber Expertise.

Dr. Vilma Tomco is director-general of the National Authority for Electronic Certification and Cyber Security at the Council of Ministers of Albania. She holds a Ph.D. in information systems and has worked in the telecommunications sector for 24 years. From 2013 to 2017 she was director of the European Information and Communications Technology Agenda Department at the prime minister's office. The department contributed to the development of digital and innovation policies, public administration reform, realization of national digitalization objectives and improvement of public services.

Jelica Vujadinović is security advisor in the Serbian National Computer Emergency Response Team. She focuses on handling cyber security incidents on the national level, analyzing vulnerabilities and risks in order to raise public awareness, and on training relevant cyber security stakeholders. She has participated in creating Serbia's cyber security policies.

Clemens Woywod has 24 years of international experience as a researcher and teacher in theoretical chemistry and biology. He also has expertise in the development and application of scientific software, a background in system administration and high-performance computing, and experience in administrating scientific projects. He's conducted research in Germany, Norway and the United States.

Cyber Workforce Development

TO MEET TODAY'S NATIONAL DEFENSE CHALLENGES

By **Tom Wingfield**, OSD(P)/HD&GS/DASD for Cyber Policy

Famed German-born scientist Albert Einstein was once asked how, if he had one hour, he would go about saving the world. After a moment's reflection, he said that he would take fifty-five minutes to define the problem, and the last five minutes to solve it.

We are now framing the problem of how to ensure that the most important part of the cyber ecosystem — the human component — is prepared to design, build, maintain, operate, and defend our cyber infrastructure. Despite the clarity of need, the scarcity of skilled cybersecurity thinkers and workers remains a well-documented global challenge for industry and for governments alike. Certainly, some sectors lag behind, but most government and industry leaders are now cognizant of and attentive to the need for increased security and resiliency in cyberspace.

Accepting cybersecurity skills were both scarce and unevenly distributed, even in the U.S. national security sphere, President Trump issued an executive order in May 2019 to jumpstart federal cybersecurity workforce enhancements. "The Nation is experiencing a shortage of cybersecurity talent and capability, and innovative approaches are required to improve access to training that maximizes individuals' cybersecurity knowledge, skills, and abilities," he wrote. Further to that point, the recently published Executive Summary of the Cyberspace Solarium Commission, a bi-partisan, Congressionally-chartered commission, stated that "Congress and the executive branch should pass legislation and implement policies designed to better recruit, develop, and retain cyber talent while acting to deepen the pool of candidates for cyber work in the federal government."

In response to these mandates, the United States Department of Defense (DoD) — with over 1.4 million active duty personnel, 1.1 million reservists, and 861,000 civilian employees stationed in the United States or overseas across 163 countries — understands cybersecurity is a critical component to achieve its missions, and that attentive and careful development of its cyber workforce is key to its success.

For DoD, a first principle is to define the focus of effort: the Defense Cyberspace Workforce, which the Department now formally defines as consisting of "positions that are recognized as critical to the defense of the nation and is comprised of personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources to include supportive work roles; conduct related intelligence activities, enable future operations and project power in and through cyberspace."

This definition is further refined by the DoD Cyber Workforce Framework (DCWF), which serves as the authoritative reference for the Department's comprehensive approach to cyber workforce talent management that addresses military, civilian, and contracted personnel. The benefits of the DCWF are many: it implements a role-based approach for the identification and reporting of cyberspace positions for enhanced workforce planning; it establishes an enterprise-wide qualification program focused on verifying knowledge and capability, promoting continuous professional development, supporting role-based progression across the cyberspace

workforce; it sets baseline standards for the Department that do not rely on antiquated personnel structures; lastly, the DCWF Program directly supports operational needs and workforce readiness, while allowing for customization and flexibility at the Component-level.

To develop the DCWF, the DoD leveraged the National Initiative for Cybersecurity Education (NICE) Workforce Framework by the National Institute of Standards and Technology (NIST), as well as the Joint Cyberspace Training and Certification Standards issued by United States Cyber Command. This allowed the Department to build a bridge between national standards and our operational forces, and to cover a broad and varied range of cyber work roles — the DCWF contains 54 of them — and job functions.

Moving forward, DoD recognized the need for a flexible personnel system for civilians in the Defense Cyberspace Workforce. Motivated by and in synch with the 2018 *DoD Cyber Strategy and National Defense Strategy*, the Cyber Excepted Service (CES) Personnel System is designed to address acute challenges in recruitment, development, and retention of DoD's civilian cyberspace workforce. The CES recognizes the complexity of managing today's cyber workforce, offering a readily available and funded tool-set that transcends current governmental HR practice and systems. Indications are that Services which have completed conversion to the CES are leveraging these enhancements with great success in improving civilian manning and incentivizing cyberspace professionals.

The Department remains committed to supporting interagency cyber workforce initiatives, actively partnering with NIST and other federal partners to support NICE, and building resources that are shared across the federal government and at the national level. This work includes sharing best practices and lessons learned with international partners seeking to leverage NIST standards to develop training and education programs, often in cooperation with the United States. The objective in every case is to create a diverse group who govern, design, defend, analyze, administer, operate, and maintain the ecosystem of policies, systems, and networks on which our way of life depends.

As with other long-term, multifaceted challenges, education and training of the personnel working on those challenges are key components of any solution — and this is particularly true in cyberspace, which is, after all, a manmade domain. The United States, along with its allies and partners, requires a greater number of citizens — practitioners and policy-makers alike — who are properly educated and trained in cyber capabilities. Challenges posed by remote working situations during the recent pandemic, for instance, have highlighted the importance of strong cybersecurity, sound cyber hygiene practices, and broad cyber literacy. We need a capable cyber workforce to make it all work. Whether they are employed in the public or private sectors, these cyber-aware workers are the front-line guardians of our collective ability to protect national and economic security.

To grapple with cyber workforce issues is to recognize there is no single underlying problem. To further develop our respective cyber workforces, we all face an interconnected array of issues tying together primary and higher education, diversity and inclusion, industry certifications and competencies, recruitment, retention, apprenticeship and work-based learning, national hiring practices, and much more. Coordinated efforts across the entirety of a business or a bureaucracy are necessary to reverse current trends; underscoring the complexity of this challenge, solutions to fill this gap rely on input from a variety of stakeholders.

We need a capable cyber workforce to make it all work. Whether they are employed in the public or private sectors, these cyber-aware workers are the front-line guardians of our collective ability to protect national and economic security.

As such, any discussion on cybersecurity workforce development is a network of conversations. These conversations must be conducted domestically and with like-minded international partners, and they need also to be mindful of cross-border interdependencies in cyberspace, always grounded in projections of risks and an awareness of threats. Cyber workforce improvement efforts touch upon a number of technical and occupational fields, each with its own needs and policy prescriptions, from hardware acquisition and modernization, to human resource imperatives, such as training, education, hiring, and retention. In the final analysis, such considerations should be in the forefront of the minds of leaders all over the world because a nation's cyber workforce is among its most precious strategic assets. ◻

Tom Wingfield is deputy assistant secretary of defense. He supports the U.S. secretary of defense and other senior Department of Defense leaders by formulating, recommending, integrating, and implementing policies and strategies to improve the department's ability to operate in cyberspace.

A DOUBLE DOSE
ONLINE

Read current and past issues of *per Concordiam*

https://perconcordiam.com

Submit articles, feedback and subscription requests to the Marshall Center at: editor@perconcordiam.org

Get the freshest *global security news* updated weekly:

transnational
weekly

https://www.marshallcenter.org

GEORGE C. MARSHALL EUROPEAN CENTER FOR SECURITY STUDIES
DEMOCRATIA PER FIDEM ET CONCORDIAM

ENERGIZING

A WORKFORCE ECOSYSTEM

It takes partnerships and planning

By **Danielle Santos**, program manager
National Initiative for Cybersecurity Education at the National Institute of Standards and Technology, United States Department of Commerce

As the world becomes ever more connected through technology, the need for a workforce that can protect those technologies becomes increasingly important. However, studies show that the supply of cyber security talent is not meeting demand. The cyber security workforce shortfall is well documented. The "(ISC)^2 Cybersecurity Workforce Study, 2019" estimates that the global workforce needs to grow by 145% to meet the demand of businesses today. In the United States alone, CyberSeek.org estimates there are currently over 500,000 unfilled cyber security jobs.

Further, the time it takes to hire and train employees causes lengthy setbacks for organizations. ISACA's "State of Cybersecurity 2020" report indicates that for nearly 30% of survey respondents, filling a cyber security position with a qualified candidate takes more than six months. Another 30% report that filling positions takes three months. Additionally, 70% of respondents generally do not believe their applicants are well qualified for the job. A collaborative approach to producing a workforce skilled in cyber security can help minimize these critical issues.

Public-private partnerships

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, represents a public-private partnership of academia, industry and government, whose mission is to promote and energize a robust and integrated cyber security education and workforce ecosystem. That is why NICE proudly embraces ideals such as facilitating collaboration, fostering communication and sharing resources.

NICE has been operating under a strategic plan developed in 2016. The Cybersecurity Enhancement Act of 2014 reaffirms the role of NICE, and Title IV of the act directed the NIST, as the lead agency for NICE, to develop and implement a new strategic plan every five years to guide federal programs and activities in support of the national cyber security education program. The act further directs NIST, "in consultation with appropriate Federal agencies, industry, educational institutions, National Laboratories,

the Networking and Information Technology Research and Development program, and other organizations, [to] continue to coordinate a national cybersecurity … education program" and to develop: "supporting formal cybersecurity education programs at all education levels to prepare and improve a skilled cybersecurity and computer science workforce for the private sector and Federal, State, local, and tribal government; and ... promoting initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal government and develop strategies for recruitment, training, and retention."

The NICE Strategic Plan is the result of engagement and deliberation among NICE partners in government, academia and industry. The plan outlines a vision, mission, values, goals and objectives. NICE partners will continue to develop appropriate implementation strategies, metrics and plans to announce a new five-year strategic plan in November 2020.

NICE Vision

The NICE vision is for *a digital economy that is enabled by a knowledgeable and skilled cyber security workforce*. The increasing reliance of the public and private sectors on a resilient cyberspace for the delivery of online services to citizens and consumers demands a holistic effort that includes the need for people with the necessary knowledge, skills and abilities to perform tasks that lead to increased security of data and computer networks.

NICE Mission

The mission of NICE is *to energize and promote a robust network and an ecosystem of cybersecurity education, training and workforce development*. Although the NICE acronym emphasizes education, training provides an increasingly important educational opportunity, whether provided by a commercial entity or employer. Certifications, especially when accompanied by hands-on learning and performance-based assessments, are credentials that can be used to validate knowledge, skills and abilities. NICE is also focused on developing a skilled cyber security workforce, so making sure that educational providers and employers are aligned with the NICE Cybersecurity Workforce Framework (or NICE Framework) is a priority.

NICE Values

Perhaps the most important aspect of the strategic plan development was the socialization process that led to the creation of a shared set of ideals. *Collaboration and Communication* are at the center of how NICE seeks to create a sense of community that will encourage stakeholders to *Share Resources*. We serve diverse communities and rely on thought leadership from across economic sectors, so it is important that we *Model Inclusion* in our programs and activities. We also want to be known for our ability to *Pursue Action* and get things done so it is important that we *Challenge Assumptions*, *Seek Evidence* and *Measure Results*. The challenges are immense, and the status quo is insufficient so we must be prepared to *Embrace Change* and look for ways that we can *Stimulate Innovation*. Together, as a community, we can collectively make progress to close the cyber security skills gap and enhance our economic and national security.

NICE Goals and Objectives

The strategic plan sets forth a broad set of goals and objectives designed to inform actions and determine priorities for the next few years.

Recognizing the widening gap between the growing demand for skilled cyber security workers and the available supply, the first goal is to *Accelerate Learning and Skills Development*. We must inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cyber security workers. This goal represents perhaps the greatest challenge and most critical need to identify creative and effective ways to close the skills gap. These objectives challenge us to experiment with new approaches, such as the use of apprenticeships and cooperative education programs, to move students into the workforce more rapidly. The objectives also invite us to find ways to move displaced workers or underemployed individuals into cyber security careers.

NICE Strategic Plan Goal 1

The second goal, recognizing the unique contributions of educational providers and the backgrounds of diverse learners, compels us to *Nurture a Diverse Learning Community*. The aim is to strengthen education and training across the ecosystem to emphasize learning, measure outcomes and diversify the cyber security workforce. There have been significant investments in the development of education programs, co-curricular experiences, training and certifications; however, we must work to continuously improve to make sure that those programs are having the intended impact on diversity. The Centers for Academic Excellence in Cybersecurity, led by the National Security Agency and U.S. Department of Homeland Security, and the Advanced Technological Education Centers in Cybersecurity funded by the National Science Foundation represent significant momentum to build capacity and increase participation by institutions of higher education. It is widely recognized that to sustain the pipeline needed for a robust cyber security workforce we must introduce students to career opportunities as early as possible and ensure that their academic preparation in secondary schools propels them into higher education. The under-representation of women and minorities and the under-utilization of veterans in the cyber security workforce is a well-documented concern, and we must develop concrete actions that reverse those trends.

NICE Strategic Plan Goal 2

Finally, the opportunities afforded by cyber security employment will provide an economic development boom to communities, but public sector and private sector employers need guidance to help them navigate this ever-changing career field. That is why our third goal is to *Guide Career Development and Workforce Planning*. Human resource professionals, hiring managers, and cyber security professionals require support to address market demands and enhance recruitment, hiring, development and retention of cyber security talent. CyberSeek.org, funded via financial assistance from NIST, the nonprofit CompTIA and Burning Glass International Inc., is part of the overall objective to identify and analyze data sources that support projecting present and future demand and supply of qualified cyber security workers. Additionally, the NICE Challenge Project (https://www.nice-challenge.com), developed by California State University, San Bernardino, is creating virtual challenges based on the NICE Framework tasks. The Cybersecurity Workforce Development Toolkit developed by the U.S. Department of Homeland Security is an example of a tool that will assist human resource professionals and hiring managers.

NICE Strategic Plan Goal 3

A Collaborative Approach

America's Cybersecurity Workforce Executive Order, announced on May 2, 2019, called for a "consultative process that includes Federal, State, territorial, local, and tribal governments, academia, private-sector stakeholders, and other relevant partners to assess and make recommendations to address national cybersecurity workforce needs and to ensure greater mobility in the American cybersecurity workforce." We did not have to look very far to find existing mechanisms, including the NICE Working Group.

The NICE Working Group, established in 2015, provides a mechanism by which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cyber security education, training and workforce development. The working group is led by three co-chairs, each representing academia, industry and government. The NICE Working Group is composed of six subworking groups focused on topics or audiences interested in primary and secondary school cyber security education, collegiate cyber security education, cyber security competitions, cyber security training and industry-recognized certifications, workforce management, and cyber security apprenticeships. Each of the subgroups, as well as the full working group, are open to the public.

The NICE Working Group, K12 subgroup, meets at the 2018 NICE Conference and Expo in Miami, Florida. FLORIDA INTERNATIONAL UNIVERSITY

The working group and subgroups continue to actively identify projects and produce products (one-pagers, white papers, tools, presentations, etc.) that are directly responsive to the goals and objectives of the NICE strategic plan. The working group is actively consulted for input. For example, as NICE looks to have an updated strategic plan this year, each subgroup has focused meetings to deliberate on the needs and to brainstorm themes, goals and objectives for the future strategic plan. The working group and each subgroup were also actively engaged during the summer of 2017 when NICE organized a process to respond to the requirements of the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, to include an assessment of "the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education" and "provide a report to the President with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors." The consultative process used at that time resulted in the "Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future" (Workforce Report).

Other ways that NICE seeks to consult with academia and industry include:

- Requests for information (RFI) that seek input on cyber security education and workforce topics, such as the RFI issued in response to Executive Order 13800 that requested "information on the scope and sufficiency of efforts to educate and train the Nation's cybersecurity workforce and recommendations for ways to support and improve the workforce in both the public and private sectors."
- Public comment periods are routinely used to encourage review and feedback of draft NIST publications, including NIST "Special Publication 800-181" that established the NICE Cybersecurity Workforce Framework.
- Engagement with the Information Security and Privacy Advisory Board of NIST, established in accordance with the Federal Advisory Committee Act (FACA) to advise NIST on information security and privacy issues.
- Insights from the American Workforce Policy Advisory Board, another FACA group, that provides advice and recommendations to an interagency council led by the U.S. Department of Commerce pursuant to the executive order, "Establishing the President's National Council for the American Worker."
- Other public forums or advisory boards established for other federal government departments and agencies.
- Participation in events supported by grants from NIST such as the annual NICE Conference and Expo, the NICE K12 Cybersecurity Education Conference, and the Center for Academic Excellence in Cybersecurity Symposium held each year immediately following the annual NICE Conference and Expo.
- Invitations as speakers or guests at other academic and industry meetings or events where NICE community members can listen and learn about emerging issues, opportunities, and programs of public and private sector organizations.

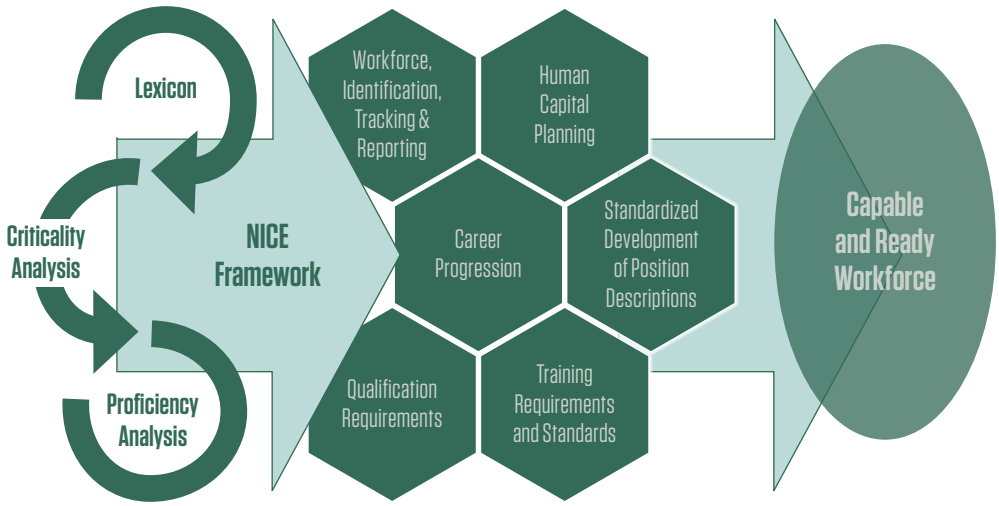
The public is invited to join and participate in the NICE Working Group by attending the NICE Conference or one of the other NICE-supported events, including cyber security education-related and workforce-related discussions at meetings or events.

NICE also engages with government organizations. The NICE Interagency Coordinating Council convenes federal government partners of NICE for consultation, communication and coordination of policy initiatives and strategic directions related to cyber security education, training and workforce development. This group meets regularly to provide an opportunity for the NICE Program Office to communicate program updates with partners in the federal government and to learn about other federal government activities in support of NICE. The group also actively identifies and discusses policy issues and provides input into the strategic direction for NICE.

A Common Thread

The NICE Cybersecurity Workforce Framework was designed to create a common language for categorizing and describing cyber security work and offer a tool for baselining capabilities, identifying skill gaps and ensuring a robust cyber security talent pipeline. The first version of the NICE Framework was published in 2012 and has become a nationally focused standard for cyber security employers, practitioners, educators, training providers and learners across public, private and academic sectors. It is also used internationally as a reference resource. As more organizations align their workforce development efforts to a common taxonomy, the result will be a more standardized cyber security workforce that can more effectively secure our networks and systems.

The most recent version of the NICE Framework was published in August 2017 as NIST "Special Publication, 800-181." This version expanded the original lexicon to include a refined taxonomy of cyber security work categories, specialty areas, and now roles. NIST "Special Publication 800-181" was also the first version to include details on the "Collect and Operate" and "Analyze" work categories and related knowledge, skills, abilities and tasks. Earlier versions redacted information on these categories due to their highly specialized and sensitive nature. This offered learners deeper insights into the



Source: NICE Program Office

A U.S. Federal Bureau of Investigation employee trained in cyber security works at a forensics lab in Louisiana, where more than 20 employees analyze hard drives and computer memories to detect and deter hackers.
THE ASSOCIATED PRESS

nature of this work and enabled educators and training providers to prepare workers in these areas.

The NICE Framework will continue to evolve with the needs of the communities that it can serve. NICE is leading an effort to dynamically maintain the NICE Framework's relevancy, applicability and utility while improving its ongoing alignment with related standards, guidelines and other frameworks. Keeping the NICE Framework relevant is vital to prepare our nation's workforce for increasingly complex cyber security challenges. As such, we began a regular update cycle and announced plans in November 2019 to publish a revision of NIST "Special Publication 800-181." Prior to publication, a draft was produced for public comment. NICE Framework updates will happen in cooperation with the private sector and other government agencies via transparent, open and collaborative processes.

Changes to the NICE Framework will be framed by lessons learned from those who use and apply it. Workforce planners, educators, training providers, employers and learners may bring forth needs for additional NICE Framework components or informative references. When we actively engage the private and public sectors on standards like the NICE Framework, we rely on and use experts from around the country — and around the globe — to improve the quality, relevance, and likely use of the end product. We learn about needed improvements by getting feedback from those who have consulted, implemented, applied or mapped to the NICE Framework. Some of these cases include performing workforce audits, developing position descriptions, creating learning outcomes, validating knowledge, skills, and abilities, and creating career pathways for learners and job seekers.

Stronger Together

In September 2016, the NICE Program Office awarded funding for five pilot programs for Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development. These programs aimed to bring together employers who have cyber security skill shortages with educators to focus on developing a skilled workforce to meet industry needs within local or regional economies. One of the requirements for the program was that each participant had to identify partnerships with at least one of the following: a K-12 school or local education agency, an institution of higher education or college/university system, and a local employer.

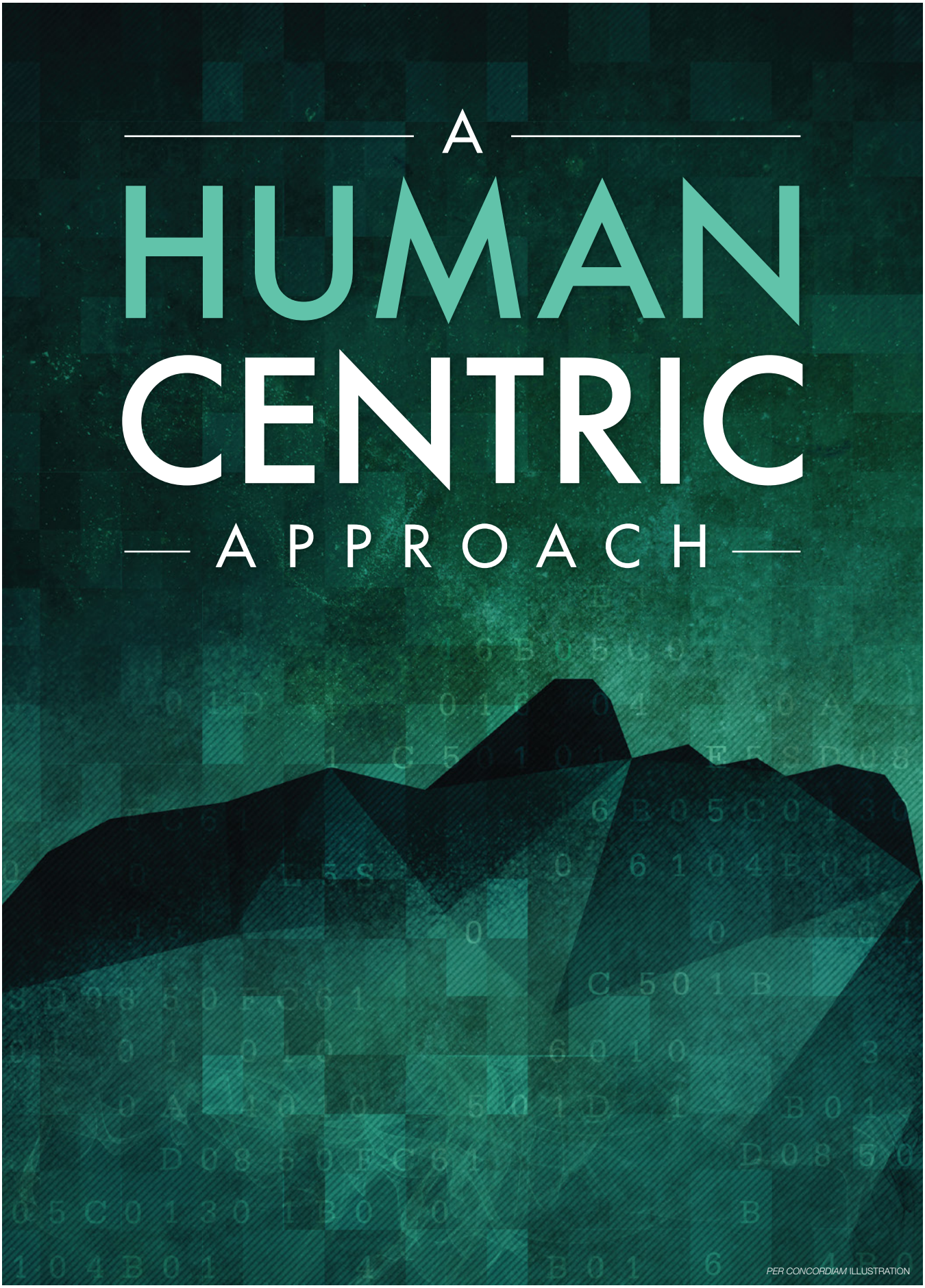
Creating these RAMPS programs showed, through metrics, that regional alliances and partnerships can have a positive impact on strengthening the cyber security workforce. Groups saw increases in student participation in courses, increases in career awareness, and more cyber security internships being secured. This evidence shows that creating collaborative environments can significantly change the cyber security workforce ecosystem. As Helen Keller put it: "Alone we can do so little, but together we can do so much."

Further Reading

The documents listed below are, by no means, a comprehensive list. However, they do provide further context on many of the programs, approaches and materials described in this article.

- NICE Cybersecurity Workforce Framework (https://nist.gov/nice/framework)
- A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce (https://doi.org/10.6028/NIST.IR.8287)
- Report on the International Workshop on Cybersecurity Education and Workforce Development Capacity Building (https://www.nist.gov/document/nice-international-workshop-report-2019)
- NICE Strategic Plan (https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan)
- Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce (https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/report) ◻

A HUMAN CENTRIC APPROACH



PER CONCORDIAM ILLUSTRATION

Portugal focuses on the individual

By **Dr. Pedro Xavier Mendonça**, **Daniela Santos**, **Isabel Baptista** and **Lino Santos**, Portuguese National Cybersecurity Centre

The term cyber security is not unambiguous. The European Union Agency of Cybersecurity's (ENISA) report, "Definition of Cybersecurity Gaps and Overlaps in Standardisation," reveals the term's different meanings among international standards institutions. It refers to the "confidentiality, integrity and availability of information" in cyberspace (the International Organization for Standardization — ISO); to "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (the International Telecommunication Union — ITU); or to "the ability to protect or defend the use of cyberspace from cyberattacks" (the U.S. National Institute of Standards and Technology — NIST). These different perspectives place great importance on protecting information and networks and are occasionally restricted to threats that come from the internet (NIST) or are open to embrace other types of threats (ITU).

We acknowledge these various definitions, but we believe that cyber security goes well beyond information security. Events such as the Cambridge Analytica scandal show that cyber security must address societal vulnerabilities presented by changes in the way individuals communicate, consume information and act. Therefore, it is important to further improve current definitions, such as the one from ITU, with a focus on humans as a central element of cyber security. The information and the networks that we seek to protect belong to humans and are a result of human will and activity. It is from this human-centered point of view that workforce development takes on added significance. The human element should not be a marginal or parallel aspect of cyber security, but rather the central element on which all others must converge. This approach should not be construed to imply a devaluation of technical aspects, information protection or systems architecture. It simply implies that these elements must be addressed from the human perspective. For example, an information system may have up-to-date malware protection, yet its architecture can still jeopardize core organizational or societal values.

A human-centric approach to cyber security also implies overcoming a national security-centric approach, which conceives of security and of cyber security from the standpoint of national territory and its essential services. This notion tends to have a realist consideration of security, pointing to threats as those objective dangers affecting national sovereignty. A human-centric approach is based on individuals and their networks standing for a humanistic and cosmopolitan concept of cyber security. Unlike realist arguments, it tends to recognize the constructivist character of security as a sphere defined by social actors' speech, in a process of securitization that elects and includes different spheres according to a perceived situation, a thesis that suits the transversal and multifaceted character of cyber security.

Workforce development must thereby conquer a central place in cyber security because it incorporates the importance of human factors, considers skills development to effectively protect individuals, and calls for strategies that seek to disseminate cyber security by identifying behavior as a vector that is a fundamental connector to other vectors.

THE PORTUGUESE STRATEGY

In Portugal, a major effort has been made toward the development of a cyber security public policy. The 2019 Portuguese National Cyberspace Security Strategy has a central role in that process, being the second strategy of that sort in Portugal after the first was launched in 2015. The 2019 strategy explicitly recognizes the importance of workforce development. This strategy has several axes of intervention. Among the most important, and certainly the one with more lines of action, is the axis concerning "prevention, education and awareness." It includes workforce development in three areas of intervention: the training and requalification of specialists, the training and awareness of leaders, and the raising of public awareness. Recognizing the transversal character of digital transformation and, therefore, its human-centric weight, this strategy promotes education and training programs that qualify and requalify workers, both within the scope of cyber security organizations and, importantly, also within the scope of the general public, the private sector and public administration, including essential services providers. It also promotes talent identification in "Capture the Flag" events and workers training in national and organizational exercises.

To define, execute and evaluate a strategy, we must identify the starting state to clearly depict the present situation, how the lines of action are being carried out, and whether established objectives are being achieved. With that in mind, the Portuguese National Cybersecurity Centre (CNCS) created a Cybersecurity Observatory that aims to respond to these needs, as well as gather knowledge about the state of cyber security in the country using a multidisciplinary method that covers various areas where the human being is key to cyber security.

Workforce development is a central aspect. The observatory defines and collects metrics about the number of cyber security courses in Portugal, people trained in cyber security, the percentage of women in these courses, the level of employment in each field in terms of supply and demand, people enrolled in nonformal training and other aspects that promote knowledge about workforce development. This knowledge is part of what can be called a "triangulation" involving research and development, knowledge and workforce development. The observatory collects and promotes research and development, disseminating knowledge that may be used to provide tangible outcomes for society by creating, for instance, workforce development programs.

EXERCISES, AWARENESS AND TRAINING PROGRAM

Some of the most central aspects of the CNCS' strategy for workforce development are exercises and the Awareness and Training Program that are promoted or carried out with stakeholders. Exercises are held annually, and each seeks to train key employees from critical organizations in a given situation. For example, in 2019, during which three elections were held in the country, an exercise on this topic included hypothetical disinformation campaigns. For this purpose, several entities were involved, including the National Elections Commission and the Portuguese Regulatory Authority for the Media. The sharing of commonly created experiences at this level has made it possible to better prepare professionals to respond to cyber-related incidents during elections while promoting the transference of knowledge to those organizations.

The Awareness and Training Program is key in developing the skills of workers and managers. It is planned to deepen the training for specialists in the program but that aspect remains, for now, primarily under the umbrella of the cyber security frameworks and tools promoted by CNCS. A draft of the Awareness and Training Program was presented to a community of educators, researchers and business institutions. The final project integrated suggestions from this community that focused on three models of action: Massive Open Online Courses (MOOCs) in cyber security for all workers, but also for specific institutions; Train the Trainers, in which, by training and validating trainers from different organizations, the training capacity is raised and disseminated; and face-to-face awareness and training sessions for the general workers and senior-level leaders.

In 2019, the Cybersecure Citizen MOOC was created. This is a free and simple course with recommendations on cyber-hygiene practices that targets common citizens as an intersecting workforce. During its first year, more than 30,000 citizens participated and about 20,000 completed the course successfully. Based on their feedback, concerns and needs, the themes of the next MOOCs were defined: disinformation, online shopping and safe behaviors on social media.

The Train the Trainers model requires the collaboration of workers — mainly from public administration and large companies — who become part of a pool of trainers who can use CNCS materials to conduct cyber security training sessions in their organizations. This model was presented to all stakeholders as a social responsibility with no associated costs. As it is an essential service and the target of many cyber attacks, the health sector became involved very early and with great commitment. For similar reasons, the Tax Authority was likewise an important partner. Universities are of great importance because they are more conscious of the need to raise awareness and train their school communities, as well as the local communities, of which they are a part. In more inland parts of the country, these institutions play a very important role in economic and social progress, as well as in workforce development.

Regarding formal education, CNCS helped in the creation of a vocational course with several stakeholders that is called Cybersecurity Technician. Based on the needs detected within the sphere of the computer security incident response team's National Network's activities, CNCS is also preparing postgraduate and specialization courses (online and offline) with the most updated content demanded for workforce development in this field of knowledge.

FRAMEWORKS AND TOOLS

Another important base of CNCS' workforce development strategy is the clear sense that autonomous and independent organizations should be encouraged to take the steps needed to achieve the highest possible cyber security maturity level. With that in mind, CNCS has developed frameworks and tools to guide all organizations — from the first steps to the highest levels — in their cyber security compliance. The National Cybersecurity Reference Framework is one of those documents and perhaps the most important. Based on international benchmarks, such as ISO 27001 or NIST SP-800-53, it gives clear indications about what an organization should do to identify, protect, detect, respond to and recover from incidents while adapting to the national reality and considering contributions from other international standards. Workforce development is one of the goals, with suggestions referring to the Awareness and Training Program and to additional training needs addressed by the market. To address first steps regarding workforce development, CNCS provides its Roadmap for Minimum Capacities in Cybersecurity, which allows entities with very little maturity in this field to achieve cyber security minimums. This document is especially important for small and midsize organizations with few resources available for cyber security.

CHALLENGES AND RECOMMENDATIONS

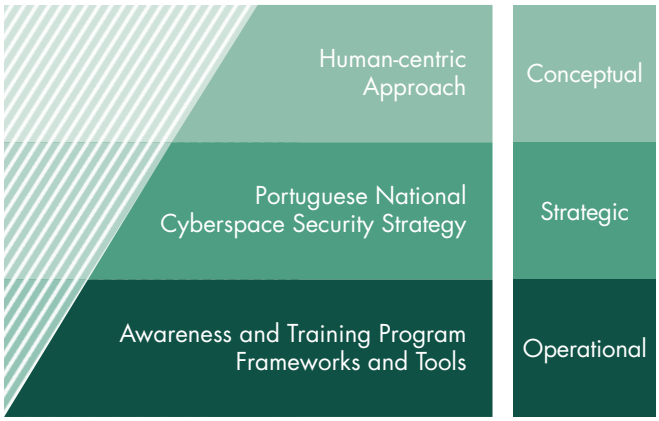
The CNCS' approach starts at the conceptual level, moves to a strategic one, and finishes with operationalization in two domains of action: training and frameworks for autonomous action. These domains must be articulated. That is, the training must reflect the frameworks, and the latter must include training as part of the compliance process.

The most success to date has been with the dissemination capacity that the Awareness and Training Program

Vocational facilities, high schools and universities must understand the importance of introducing cyber security subjects and content in all IT teaching programs.

ISTOCK

FIG. 1 - CNCS' WORKFORCE DEVELOPMENT STRATEGY



revealed, showing a civil society eager to adopt these types of activities; additionally, there has been success with the dynamics of framework building, which included the participation of several stakeholders and a very interesting adaptation of international standards to the Portuguese context. This had the augmenting effect of hardening the network of stakeholders, hence contributing to the strength of the whole.

One of the main challenges faced in workforce development is the need to create more training for technicians, responding to the demand imposed by emerging technologies, as well as the strong need for requalification of information technology (IT) professionals for cyber security. Another major challenge is to persistently articulate to vocational facilities, high schools and universities the importance of creating more courses and introducing cyber security subjects and content in all IT teaching programs. In vocational education and high schools, it is also critical to introduce cyber security content to raise awareness and to spark interest in the youngest so that they may identify a possible vocation in this field. Moving from frameworks to practice is also a considerable challenge. Considering the limited resources available, this aspect needs major contributions from the market and from civil society.

To apply the best workforce development practices, national cyber security authorities should involve all stakeholders as much as possible. This is for two reasons: because stakeholders, more than anyone else, know how to identify their needs, and because their involvement motivates and holds each one responsible, promoting quality of output. Among the stakeholders, it is essential to include spokespeople from academia, as well as professionals and business associations. In addition, the creation of frameworks must include workforce development in a privileged place and should include schools and training organizations to ensure the spread of specialized training and requalification.

Cyber security workforce development, as an intersecting need, should be applied using a bottom-up methodology, involving all actors that may benefit from it. From this point of view, it must put humans at the center of its approach, hence enabling security, including cyber security, to have the real scope it deserves, i.e., contributing to safer and more prosperous lives for all humankind. ◻

INCENTIVIZING

PRIVATE ENTITIES

HOW GOVERNMENT PROCUREMENT CAN BOOST CYBER SECURITY

PER CONCORDIAM ILLUSTRATION

By **Atsuko Sekiguchi**, deputy counselor, International Strategy Group, National center of Incident readiness and Strategy for Cybersecurity (NISC), and cabinet secretariat, government of Japan

Workforce development in the cyber security sphere is an urgent issue in Japan and across the world. According to the "(ISC)² Cybersecurity Workforce Study, 2019," the global shortage amounts to over 4 million workers. In the Asia Pacific area, the shortage is 64% of need. In Japan, the Asian-Oceanian Computing Industry Organization reported in 2018 that the shortage of capable talent reached 132,000 in 2016 and was expected to increase to 193,000 in 2020.

Out of respect for the autonomy of private entities, workforce development policy in Japan is implemented through voluntary initiatives. For instance, the cyber workforce has been developed under the 2018 Cybersecurity Strategy by raising awareness, enriching opportunities for education and capability development during careers, and the promotion of a certification system.

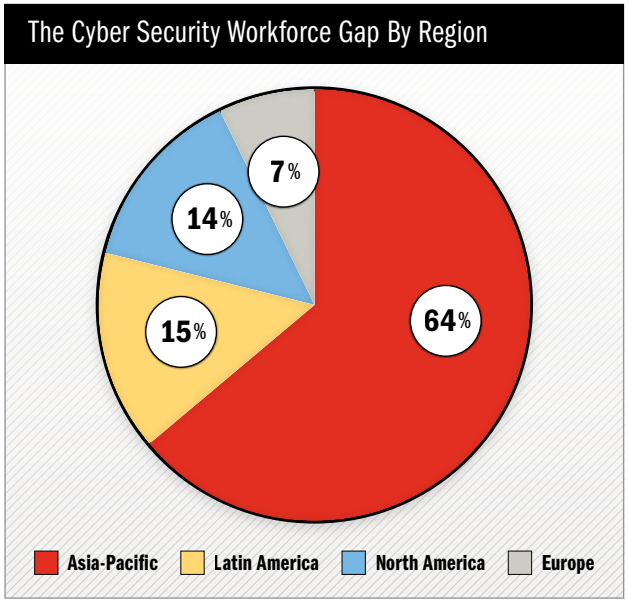
Yet, an insufficiency in the number of capable workers is widely recognized, showing the limitations of voluntary initiatives. One consideration for the enhancement of policy implementation could be an introduction of obligatory measures, such as the path taken in the United States, where the Executive Order on America's Cybersecurity Workforce issued in 2019 has been implemented. The order requires entities that participate in government procurement to deploy the National Initiative for Cybersecurity Education (NICE) framework that visualizes cyber security-related roles and encourages the career development of practitioners.

The first part of this essay explains current policy of workforce development for private entities in Japan and current data regarding the cyber security workforce. The second part shows the case for an obligatory effort to encourage workforce development, as deployed in the U.S. The last part is an examination on the applicability of this U.S. measure in Japan, resulting in a proposal suitable for the Japanese system.

THE SITUATION IN JAPAN

The historical basis of cyber security policy in Japan was the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society, passed in 2000, with Article 22 imposing a general obligation on the government to take measures to ensure security in telecommunications networks, which means that information security was merely a part of the legislation on the acceleration of digitization and that there was no reference to relevant stakeholders.

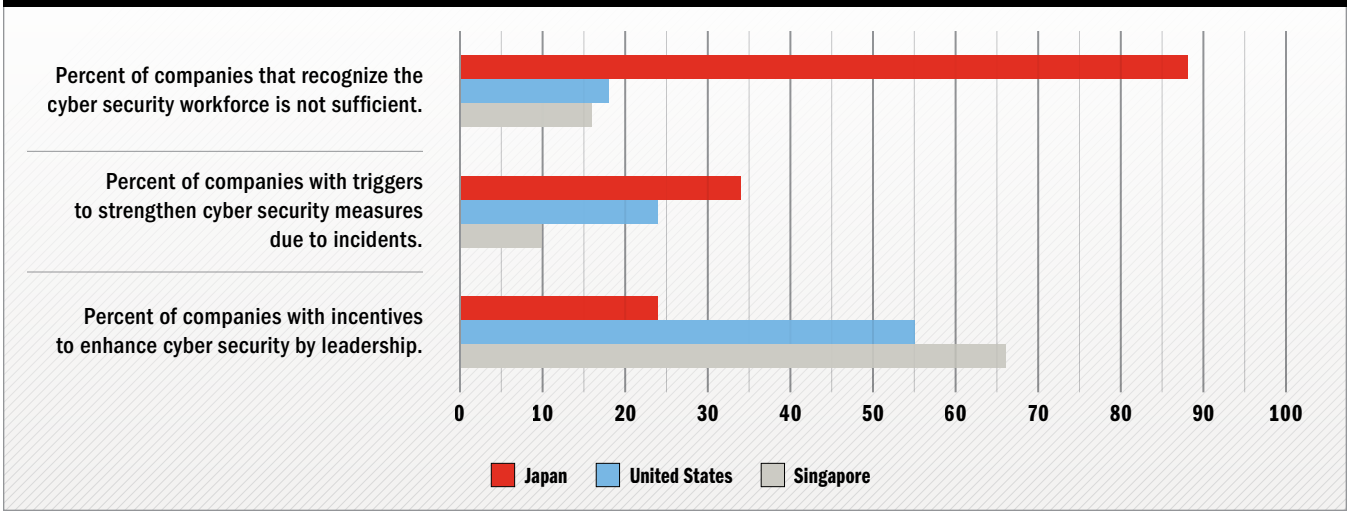
Japan's current cyber security policy stems from the Basic Act of Cybersecurity, passed in 2014. In that act, Article 4 requires the government to create and implement cyber security policy across the nation. Articles 6, 7 and 8 set the responsibility of critical infrastructure operators, private entities and cyber-related private organizations to cooperate with the government to achieve the goal of a national cyber security policy. Article 22 specifically requires the nation to take the necessary measures for workforce development in cyber security by ensuring appropriate rewards for professionals, utilizing certification systems, and providing education to the young via cooperation with educational institutions and private entities. This means that the law sets the responsibilities for each stakeholder relevant to workforce development, yet, respecting the autonomy of nonpublic organizations, it is not obligatory for private entities.



Source: "Cybersecurity Workforce Study" in 2019 issued by (ISC)²

The responsibility of the government is legally stipulated, yet specific measures are not stated within the legislation. As such, the Cybersecurity Strategy and related documents specify the direction of cyber security policy. The legislation requires that the Cybersecurity Strategic Headquarters (CH) be established as the highest authority of decision-making on cyber security policy, composed of

Comparison of Recognition Toward Cyber Security Among Japan, the U.S. and Singapore



Source: "NRI Secure Insight 2019"

relevant political figures, academics and private professionals, and it tasks the CH with setting cyber security strategy. Cybersecurity Strategy 2018, the most current, has three pillars: economic vitality, security of society and international stability. One section is devoted to workforce development as a cross-cutting measure supporting the pillars. The section points out that it is necessary to implement policy at all levels — in private entities, educational institutions and government. Related to the strategy, the CH instituted the Cybersecurity Workforce Development Initiative in 2018. The specific measures toward private organizations in this program are: changing the awareness of executives by disseminating the cyber security policy guidelines; providing opportunities for workers to reskill themselves and to develop their professional careers for management positions; and building technical capacity through a certification system. Therefore, the direction of the workforce development policy toward private entities is to create the appropriate environment to develop their awareness and skills.

In addition to statistics that show an estimated increase in Japan's workforce shortage, the "NRI Secure Insight 2019" study shows that 87.8% of companies in Japan recognize that the cyber security workforce is insufficient, while that same indicator is 18.1% in the U.S. and 16.3% in Singapore. The government of Japan has taken measures for workforce development by capacity building and educational opportunities, but there remains a wide recognition of deficiency.

Although the Japanese government is implementing policies to raise awareness within private entities, the NRI data shows that the motivation to raise the level of cyber security stems from actual damage from incidents, rather than leadership at the executive level. This raises questions about the current voluntary initiatives and whether they are sufficient to solve the inefficiency of human cyber resources in private entities.

THE U.S. EXAMPLE

The U.S. uses obligatory policies to enhance workforce development in cyber security. There are many projects within the private sector that follow three goals from the 2012 NICE Strategic Plan: Accelerate learning and skills development; nurture a diverse learning community; and guide career development and workforce planning. This was followed by the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure in 2017, which requires the secretary of Commerce and the secretary of Homeland Security to report on workforce development. One of the undertakings is the implementation of the NICE Cybersecurity Workforce Framework ("Special Publication 800-181") by the National Institute of Standards and Technology (NIST), which is part of the U.S. Department of Commerce, in order to visualize the capability of the cyber security workforce. The framework categorizes types of work into seven genres: security provision, operate and maintain, oversee and govern, protect and defend, analyze, collect and operate, and investigate. Within that, 33 specialty areas and 52 work roles are mapped. Additionally, at the regulatory level, the Executive Order on America's Cybersecurity Workforce, introduced in 2019, requires private entities that participate in government procurement to apply the framework within their organization in order to promote its utilization.

JAPAN AND THE OBLIGATORY APPROACH

Would the obligatory approach in the U.S. be appropriate in Japan? Regarding mapping capacity in the area of cyber security, the Cyber Risk Intelligence Center-Cross Sector Forum produced a Reference of Definitions of Human Resources in collaboration with the U.S. NICE. The forum is composed of several dozen indigenous companies and foreign subsidiaries from the chemical,

financial, manufacturing, media and transportation sectors. The reference outlines the tasks required to ensure cyber security, who is responsible for each task, and the level of knowledge necessary. The process of creating the reference enabled a common understanding of cyber security talents across sectors that have differing cultures and a varying use of terms on human resource development. Thus, Japan's framework on workforce in cyber security has been created by a private-driven organization and not by the government out of respect for the autonomy of private entities.

A website chronicles the successful collaboration between Japan's Cyber Risk Intelligence Center-Cross Sector Forum and the U.S. National Initiative for Cybersecurity Education, or NICE. NIST

The Common Standards for Information Security Measures for Government Agencies and Related Agencies (Common Standards) was established by the National center of Incident readiness and Strategy for Cybersecurity (NISC) based on Article 25 as a mandate from the CH to set a standard to evaluate measures taken by government agencies. Based on the documents, agencies set their own cyber security standard, and the NISC audits them to check whether the Common Standards are compiled regularly to ensure a certain level of security in government agencies. Section 4 imposes conditions that should be included in the government procurement process. Although the Common Standards contain technical conditions to prevent vulnerabilities within contacts between government agencies and private entities, the criteria do not include a condition on workforce development within private entities.

In summary, there are differences between the U.S. and Japan. In the U.S., a framework has been adapted within the process of government procurement to force private entities to accept the framework within their organizations. On the other hand, in Japan, the condition of government procurement does not involve the implementation of workforce development policy by private entities. Furthermore, although workforce mapping suitable for Japan's culture was produced, its application remains at the level of initiatives by private organizations. Thus, it is difficult and not appropriate to introduce the policy implemented in the U.S. to Japan, as many differences exist.

Additionally, requirements regarding workforce development pertaining to private entities within government procurement might lead to a discussion on whether this additional condition is allowed under World Trade Organization procurement provisions that cover nonessential conditions. The provisions limit the imposition of participatory conditions based on "legal and financial capacities and the commercial and technical abilities to undertake the relevant procurement." It remains an issue whether a workforce development requirement would comply, yet that question is not for this article to consider.

Although the deployment of the Reference of Definitions of Human Resources as an eligible requirement might not have been smooth in Japan, the government is able to carry out a comparative examination of applications from private entities in government procurement to ensure the quality of procured services. This involves several evaluative points, including the bidding price, the quality of a proposal and relevant experience to prioritize a bidder in terms of public interest. If workforce development measures, such as the deployment of the human resource framework, become part of the evaluation criteria in government procurement within the Common Standards, it will encourage private entities to make it a priority. It will also leave no doubt about conformity with the international trade regime as it encourages measures to be taken but does not exclude any entities to enter government procurement. In addition, it surely promotes the acceleration of workforce development measures within private entities beyond voluntary initiatives, and still respects the autonomy of the private sector, a principle of cyber security policy in Japan. Some might criticize the idea because the companies that can participate in government procurement do not amount to a large percentage of the nation's entities. However, it would be realistic for the government, as a first step, to incentivize private entities to deploy workforce development measures by making it one of the evaluation criteria within government procurement in the Common Standards. Furthermore, the proposal has the possibility to be expanded to other entities associated with the entity that participated in the government procurement.

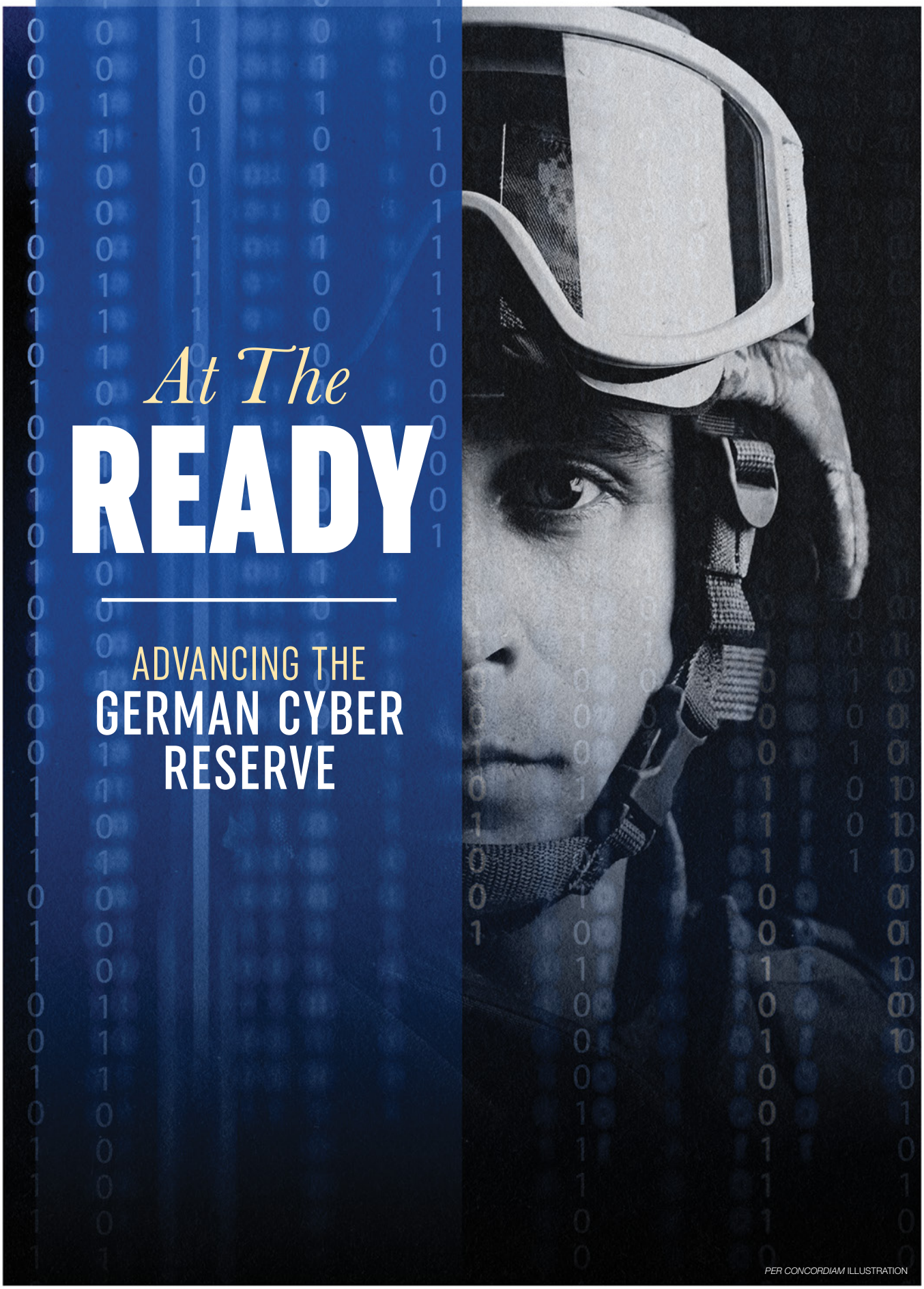
CONCLUSION

One of the possible measures to incentivize private entities in Japan is to implement workforce development plans through a government procurement process, not simply by voluntary initiatives. The proposed solution might not be perfect for covering the whole of private entities immediately. Yet, this proposal will contribute to the discussion not only in Japan, but also in other nations on how a nation can take one step forward from voluntary initiatives in the area of cyber security workforce development to improve the situation for future generations. □

This article represents the author's views and not the position of the NISC, nor the government of Japan.

At The READY

ADVANCING THE GERMAN CYBER RESERVE



PER CONCORDIAM ILLUSTRATION

By **Rupert Brandmeier**, **Jörn-Alexander Heye**, **Dr. Florian Rupp** and **Clemens Woywod**, military reserve officers, German Cyber and Information Domain Service

Tensions between the Western and Eastern political blocs decreased rapidly and substantially after the demise of the Soviet Union in 1991. Consequently, politicians in the reunified Germany increasingly questioned the rationale of compulsory military service until it was finally paused and quasi-disestablished in 2011. Thereafter, the Bundeswehr became an all-volunteer army, which has since been faced with the mounting challenge of finding sufficient numbers of appropriate recruits. Hence, the goals of increasing the importance of the reserve force and of shifting responsibilities from active service members to reservists have gained popularity in recent years. A primary building block of the pertinent master plan of the Ministry of Defense (MoD) is the deployment of an efficient cyber reserve.

The Military Information and Cyber Domain Service (MCS) is in charge of organizing all aspects of the cyber reserve. The MCS is the youngest branch of the military part of Germany's federal defense force, which also includes the Army, Navy, Air Force, Joint Support Service and Joint Medical Service. It is responsible for the cyber, information technology (IT), military intelligence, geoinformation and operative communications units. Unlike the traditional branches of the military, the MCS can act largely autonomously.

The MoD's 2016 "Report on Cyber and Information Domain" addresses the key pillars of the military cyber reserve by formulating three primary goals:

1. The creation of additional forces that can temporarily support the MCS in the case of large-scale cyber attacks.
2. The building up of strong cyber units consisting of IT experts through mutual exercises and grouping.
3. Increasing cooperation and dialogue between IT experts of the private, public and military sectors.

Then-German Defence Minister Ursula von der Leyen speaks at a ceremony in Bonn in 2017 to launch a new cyber defense unit dedicated to thwarting and responding to cyber attacks. THE ASSOCIATED PRESS

To strengthen the cyber defense, the MoD recognized the importance of qualified personnel. To attract qualified recruits to the active military and the reserve, the Bundeswehr builds on three components centered on education: a new cyber security program offered at the Bundeswehr University; separate recruitment track opportunities for computer specialists who are not following the traditional military career pattern; and an increased integration of reservists, IT experts in particular. The last two components represent a challenge because of the heterogeneous structure of the distribution of IT know-how, both in society and in the pool of reservists. Moreover, MCS cadre and experienced reservists can reach the public through talks, panel discussions and other events in order to spark interest in either active MCS careers or in joining the cyber reserve. Trial military exercises at MCS units can also be advertised.

CYBER DEFENSE **STRUCTURE**

In an April 2020 study, the ETH Zürich's Center for Security Studies compared the cyber reserve forces of Estonia, Finland, France, Israel, Switzerland and the United States. The ETH study found that the organizational forms of cyber reserves vary significantly due to the different bureaucratic and military cultures. Although France, the U.S. and the Netherlands have voluntary armies (like Germany), the preconditions for establishing a cyber reserve are rather different due to peculiarities in the educational systems, military structures and labor market landscapes.

In Germany, the setup of a new cyber reserve is tied to the establishment of regional branches of the MCS. In addition to MCS' reserve headquarters, four regional reserve outlets distributed across Germany will be expected to improve connectivity to the local cyber reserve landscape. Located in areas populated by IT specialists, the outlets are to be staffed by experienced reservists serving in rotation. This concept provides regional and local cyber expertise that may otherwise not be at the disposal of the Armed Forces.

Then-German Interior Minister Thomas de Maiziere stands before a map in 2017 showing the number of cyber attacks over a 30-day span.
THE ASSOCIATED PRESS

Another benefit of decentralizing the MCS reserve is becoming evident during the present COVID-19 pandemic: the geostrategic factor. Regular and reserve units in certain regions may be unable to perform their tasks at the necessary level of effectiveness, while such shortfalls may not affect other parts of the country. Assignments can be transferred to an MCS outlet that is fully operational and can be staffed by additional reserve members to compensate for any inefficiencies.

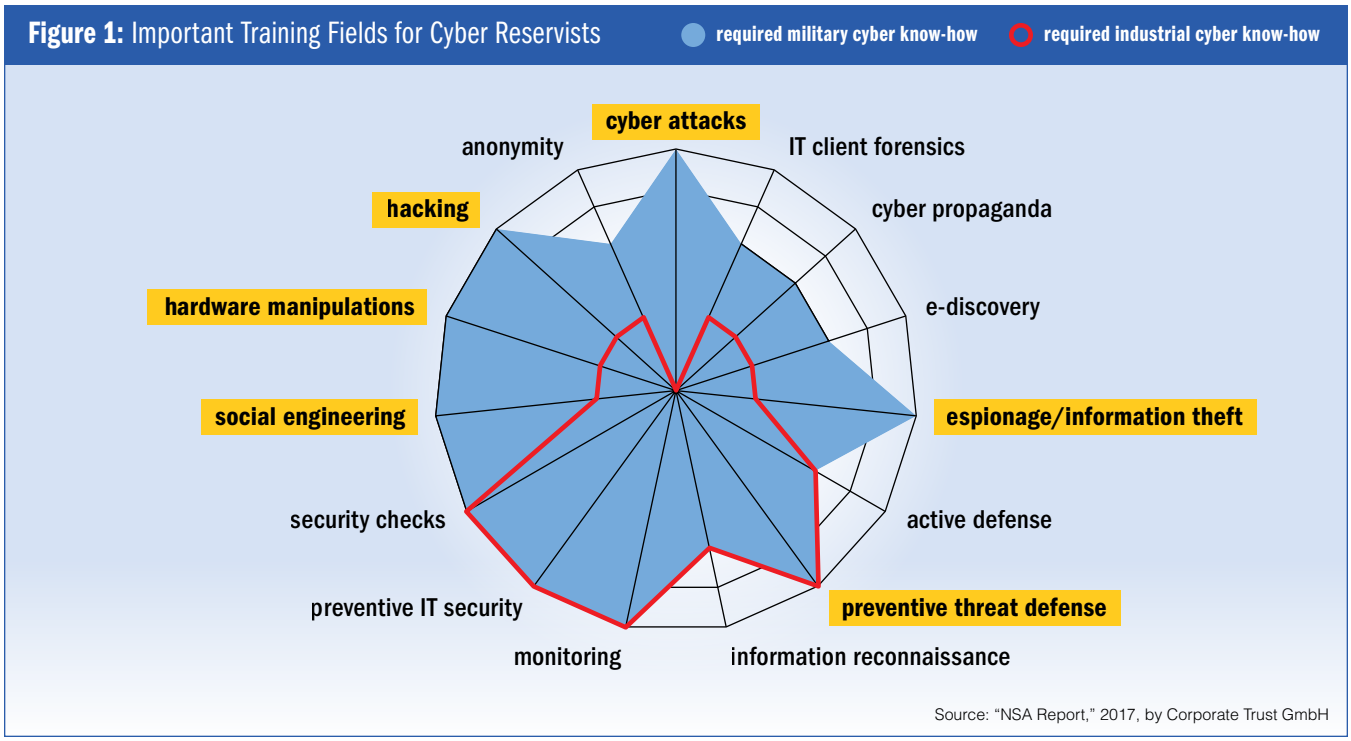
Considering the MoD's primary goals, the tasks of an MCS reserve outlet start with the allocation of attractive training opportunities for reservists together with the preparation, realization and analysis of cyber exercises, both from a curricular (such as contents) and a logistical perspective. This includes the organization of on-site and online cyber security competitions to gain the attention of computer-oriented talents and to stimulate their interest in military careers. Specific hardware and software components (such as a cyber range) will be needed to support the courses and exercises. MCS initially proposes that each cyber reservist, based on their IT background, can qualify for one of five major fields:

- **Red Team:** hacking simulations to test the resilience of computer infrastructure.
- **Cyber Intelligence:** gathering information about threats to reduce cyber risks.
- **Monitoring:** surveillance of networks, users and websites to identify failures and threats.
- **Open Source Intelligence (OSINT):** screening public internet sources for information.
- **Digital Forensics and Incident Response (DFIR):** examining digital components to identify illegal activity and implement a proper response in cases of proven cyber crime.

Other fields, such as those connected to the geoinformation tasks of MCS, may be identified in the future. Each outlet will identify the required skills potential reservists will need for a particular area of responsibility and will compile the qualifications of each reservist. Together with MCS headquarters, the outlets will develop general and individual qualifications for cyber reserve members. Once a reservist has been selected for one of the five fields, MCS will outline an individual training plan to develop the reservist into an expert.

When cyber incidents occur, the experts in each of the five fields should join their complementary expertise. Such a mitigation of cyber risks and the ability to cooperate can be tested in cyber security competitions. In addition, the cyber reserve should supply expertise in system administration, in the evaluation of the reliability and resilience of hardware and software products, in the installation of a secure network and in the protection of existing IT infrastructure. It should be familiar with organizational and communications aspects (public relations), be able to identify fake news, and be sensitized to issues of information security awareness. Finally, the reserve outlets cooperate with related organizations like the Bundeswehr Command and Staff College (Führungsakademie), Bundeswehr University, police academies and also with civilian institutions on all aspects of the cyber education of reservists. In particular, the outlets organize public events such as talks promoting the opportunities offered to prospective candidates by joining MCS or the cyber reserve.

The performance of the MCS reserve system can be challenged in national, international, or private-public-military cyber security competitions, which may feature capture the flag challenges, threat-hunting tasks, penetration-testing exercises and attack/defense simulations.



Cyber reservists will receive training in the areas of cyber attacks, espionage and information theft, preventive threat defense, social engineering, hardware manipulations and hacking.

While some problems constructed for competitions are designed to be solved by individuals, others are supposed to be tackled by teams composed of experts with specific abilities to distribute assignments.

RESERVE TRAINING **CONCEPT**

The military cyber reserve's essential role is to provide units that can be activated rapidly to compensate for Bundeswehr personnel shortages during a military crisis (including cyber aggressions). One reason for the difficulty in recruiting sufficient active military cyber personnel is that about 30 other federal and state cyber authorities — such as the federal office for IT Security and the cyber security branches of state and federal criminal investigation offices — are relying on the same experts.

The private sector adds to the difficulties. Figure 1 compares key capabilities of cyber staff working on industrial and military cyber challenges. The 2017 publication, "NSA Report," from Corporate Trust, a German risk management company, has the detailed description of these capabilities. Monitoring, one of the major fields, is highly relevant to the industrial and military sectors. This means that MCS will try to motivate industry experts in this field to join the monitoring squad of the cyber reserve. A successful recruitment of monitoring experts will not need significant training because industry and military requirements in this field are similar.

Additionally, a big part of the "required military cyber know-how" cannot be recruited from the private sector because it simply is not available. For instance, it is difficult to find experts for the Red Team (or hacking squad) in industry. The need for proper continuous education and training of cyber reservists is obviously important. In particular, the education of Red Team members will represent a substantial challenge because hacking is neither a proper job description nor do any educational pathways yet exist.

Based on an analysis of desired capabilities and available resources, targeted courses can be developed and various deployment-oriented roles and ability profiles for the assembly of specialist teams can be defined. In the context of the five expert squads, from which the specialist teams will be formed, it should be pointed out that it is sufficient for members of a given squad to acquire purely theoretical knowledge in some of the 15 cyber areas defined in Figure 1, while acquiring practical computational experience, on top of a solid theoretical foundation, is essential in certain critical areas.

Table 1 provides for the five expert squads an exemplary assignment of theoretical and practical competences in six selected, representative cyber areas.

It is important that objective, verifiable criteria be used to assess available capacities. For this purpose, each cyber reservist will undergo a cyber fitness test before entering the training program. Analysis of the deviations between required and disposable qualifications allows for determining the number of participants, the curricula, location and timing of individual courses.

As already indicated, the training of Red Team members will be of particular relevance since it will be difficult for the cyber reserve to recruit candidates with expertise in offensive methods at a sufficiently high level.

Germany's government headquarters in Berlin were hacked by a Russian-backed group that infiltrated the secure computer networks in 2018.
THE ASSOCIATED PRESS

Figure 2 illustrates an example program based on which the MCS may configure a training schedule for a prospective Red Team member.

In this example, after completing the training program, the reservist should be an expert in three branches of "hacking science" of particular relevance: web exploitation, reverse engineering of software and binary exploitation. According to the example provided in Figure 2, this individual would require an upgrade in web exploitation and reverse engineering, while no immediate education in binary exploitation would be necessary.

Pathways are provided for the training of Red Team aspirants to become proficient in the three domains. In web exploitation, trainees need to reach expert level in penetration testing, i.e., in simulated cyber attacks to check for exploitable vulnerabilities of a computer system. In introductory theory courses, inexperienced attendees will be made familiar with KALI Linux and a selection of the more than 600 offensive tools offered by this platform. In the next step, apprentices will participate in tutorials demonstrating how KALI Linux tools can be applied to solve tasks supplied by the "Hack the box" server. To reach the next level, workshops, both featuring lectures and practical exercises, will address the solution of capture-the-flag challenges maintained by the security training tool Open Web Application Security Project Juice Shop.

Key for reverse engineering of software is the analysis of software to extract design and implementation information. To qualify for training in this field, a familiarity with Java and assembly is a precondition. In introductory courses, lectures on reversing and patching machine code and Java bytecode will be combined with tutorials. Follow-up workshops will demonstrate, both in theory and practice, how reverse engineering skills can be used to mitigate malware risks.

Finally, in binary exploitation, the subversion of binary code has the goal to access protected information. This is generally an advanced topic and an intermediate level in a programming language, like C, and assembly is mandatory to qualify for a preparation course. Here, lectures will first cover vulnerable

Table 1

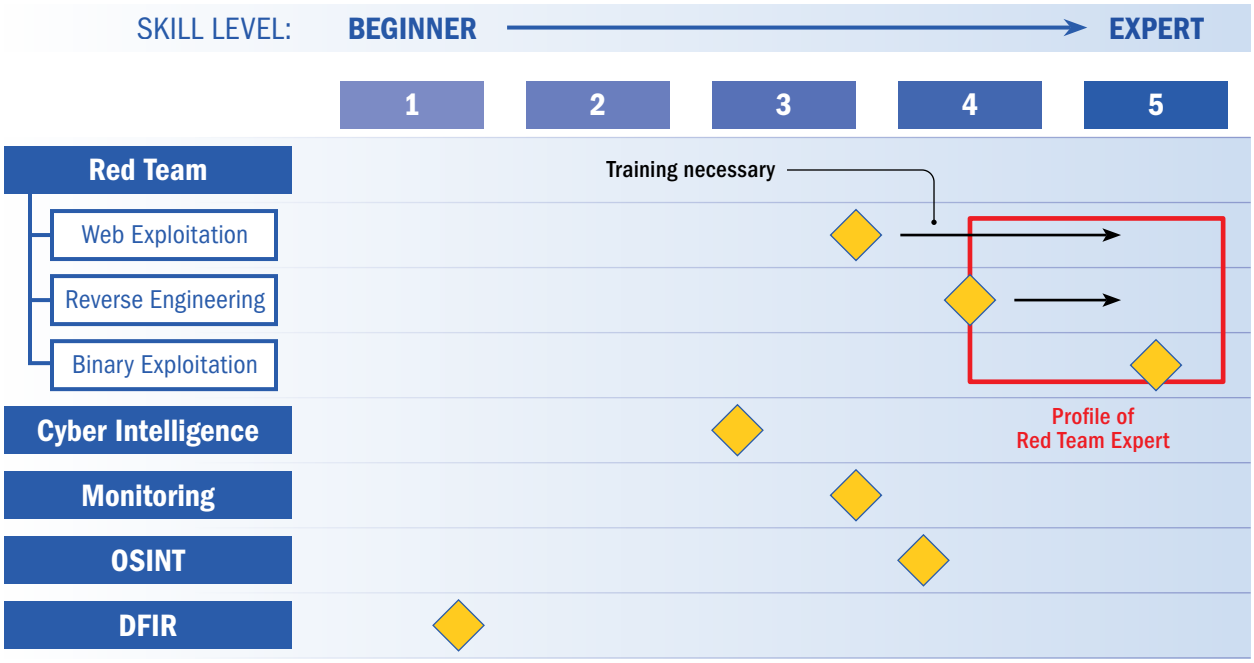
	Hacking	Cyber Propaganda	Monitoring	Active Defense	Hardware Manipulation	Espionage / Information Theft
Red Team	P	T	T	T	T	T
Cyber Intelligence	T	P	T	T	T	P
Monitoring	T	T	P	T	T	T
Open Source Intelligence	T	P	T	T	T	T
Digital Forensics Incident Response	T	T	T	T	P	P

T = theoretical competence **P** = practical competence

Source: Authors

This overview differentiates for members of the cyber reserve squads between practical (P) and theoretical (T) competences in six of the 15 cyber areas included in Figure 1. Theoretical competence in an area can be acquired by attending lectures covering subjects related to this area. Attaining practical competence in an area requires both theoretical background and actual computational experience.

Figure 2: Determining An Individual Training Schedule



Source: Authors

In this representation of a program for determining a training schedule, a reservist is trained to become a Red Team member, or hacking expert. Competence in hacking can be split into three subareas as shown. The initial skill levels of a reservist represented by the diamonds are determined by a cyber fitness test prior to the definition of the individual training program.

C functions, the use of simple exploits, the structure of the Global Offset Table, mitigations introduced in systems and essentials of Return Oriented Programming to avoid exploit mitigations. Next, trainees will have the opportunity to apply these techniques to binaries. Subsequently, workshops will focus on memory corruption, starting with instruction on how to exploit an overflow on Windows and proceeding to web browser exploitation. Teaching will be performed both in the form of lectures and tutorials.

CONCLUSION

The German MoD recognized in 2016 that major cyber challenges for society and the Armed Forces can be addressed by a military cyber reserve. Moreover, cyber reservists are considered to be valuable multipliers of cyber awareness in society. The MoD acknowledged that reaching the goal of establishing a cyber reserve able to efficiently support MCS will require significant efforts to recruit sufficient numbers of qualified reservists and to ensure the education of members of the cyber reserve. In response to these demands, a new organizational structure of cyber defense is being developed for the purpose of integrating the cyber reserve with MCS. MCS reserve outlets will be distributed across the country to improve the recruitment of reservists and to secure the continuing education of members of the reserve force. In this article, we have outlined the plan to assemble a "model kit" of cyber experts with different specialization. MCS will tap this pool of cyber reservists to form teams able to cope with the requirements arising from supporting MCS in improving IT security and in countering various cyber threats. ◻

A worker in Efurt, Germany, transports a ballot box. Cyber attacks on critical infrastructure systems are a major concern of countries across the world.
THE ASSOCIATED PRESS

THE NEED FOR ANALYTICAL SUPERHEROES

Addressing the nontechnical aspects of cyber threats

By **Ondřej Rojčík**
Head of Strategic Information and Analysis,
Czech National Cyber and Information Security Agency

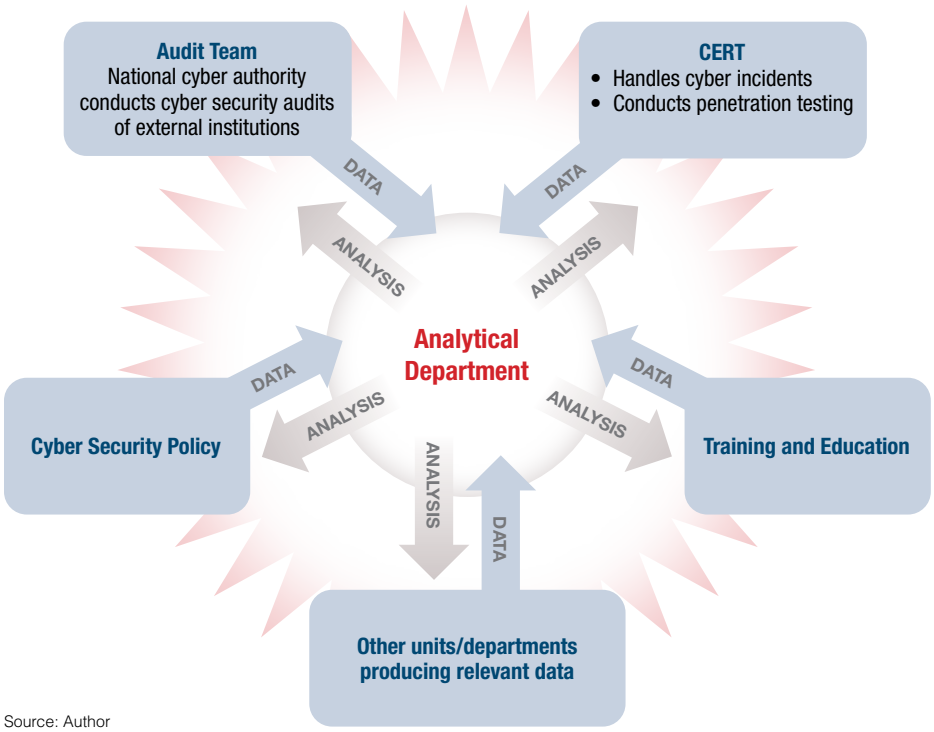
We tend to perceive cyber security as a purely technical issue. Dozens of reports from recent years point out the scarcity of cyber security experts and link this to a general lack of specialists educated in information technology. Emphasizing the relative dearth of technical talent, however, is a rather narrow perspective that doesn't account for the need for many other types of experts with backgrounds and educations that are not purely technical. For example, the labor market is seeking cyber security managers, auditors, lawyers, homeland and international security experts, regional experts, educators and analysts. Nontechnical analysts are responsible for the contextualization of cyber security incidents and trends, a function the Czech National Cyber and Information Security Agency (NÚKIB) has used in many key activities over the past four years. What skills do we need to build capability for nontechnical cyber security analysis?

Contextualization

In December 2018, NÚKIB issued a warning against using technology from the Chinese telecommunications companies Huawei and ZTE. NÚKIB reasoned that use of these companies' products constitutes a security threat because Chinese law requires Chinese citizens and companies to cooperate with state governmental agencies, including the intelligence services. As a result of the warning, system administrators of critically important systems in the Czech Republic have a legal obligation to acknowledge the threat and adopt adequate measures.

NÚKIB is also the key proponent of the Prague Proposals, a cyber security framework that emanated from the 2019 conference on 5G security in Prague. A main point of the Prague Proposals is that in addition to the technical nature of cyber threats, specific political, economic and other behavior of malicious actors should be considered when assessing the security of information technology. Cyber security has political dimensions. In the Czech Republic, experience with analysis of the nontechnical/contextual aspects of cyber security has created a strong bias toward this inclusive approach to cyber security.

The situation of Huawei and ZTE technologies and the Prague Proposals were not the first instances when NÚKIB learned of the need to develop nontechnical analytical



Source: Author

capabilities to address cyber security-related issues. Since 2015, the agency has been executing tabletop exercises for decision-makers, mainly from the government sector. One of the critical lessons learned from these exercises is that with technical data from incidents alone, without broader context, it is almost impossible for decision-makers to identify and take appropriate responses and courses of action.

In-House Analytical Capabilities

To provide contextual information and analyze the circumstances regarding a particular attack, and the legal, political and economic environment of certain actors, appropriate data must be gathered, and sophisticated analytical processes and skills must be developed. It would be very impractical to rely on external partners such as intelligence services or private companies. Intelligence services wouldn't have flexibility in two respects: First, they would rarely have the right information when it is needed. Second, most of the information would be classified, which creates difficulties in terms of immediate usability. As for private companies, it is difficult for a government organization to trust and rely exclusively on a private party and take measures based on their information. However, information from some private vendors can provide a reasonable portion of the overall data mix at a later stage of the analytical process.

NÚKIB has been building nontechnical cyber security analytical capabilities for over four years. The main function is to support NÚKIB's policy cycle and to provide analysis of cyber security issues to top decision-makers in the government and other strategic institutions. Indeed, NÚKIB is the Czech national authority in the field of cyber security. Among other activities, it is responsible for the policy and regulatory aspects of cyber security. To produce appropriate policies and regulations that reflect current issues and developments, there must be a constant state of awareness and horizon-scanning must be conducted daily. Any government institution with nationwide responsibilities in the area of cyber security would benefit from a similar capability.

NÚKIB benefits from having the technical and policy/regulation aspects of cyber security residing under a single roof. This is an effective arrangement, but for organizational or historical reasons, may not be appropriate in many countries. In many national cyber security ecosystems, these two parts of cyber security are separated, if present at all. There can be an independent national cyber emergency response team (CERT), for example, while the policy branch is under the Ministry of the Interior, Ministry of Industry, etc. If the policy branch establishes a cyber security unit within one of these ministries, it would tend to focus on strategic trends only. If it is organized by the technical branch — CERT — the natural tendency could be to stress only the contextualization of technical incidents.

In any type of arrangement, the analytical unit should not be separated from the rest of the organization. The analytical endeavor needs to spread through the organization and throughout the infrastructure (i.e., data and analytical software), including personnel. Specific units that produce relevant data should share that data with analysts who are then able to link it with data from other parts of the organization and with the broader context of external trends. Data interconnection from various parts of the organization is essential. If the data is not pooled, knowledge is contained and isolated in separate parts of the organization. As a result, the value of the data is substantially lower and the analyses inadequate.

Consider it a Project

Any organization interested in establishing a dedicated analytical unit to assess the nontechnical aspects of cyber threats must consider a plethora of factors. These include the highly specific skills of the analysts. However, these fundamental conditions should be met before any workforce development can take place.

Establishing a nontechnical analytical unit should be approached as a project. To successfully run such a project, it is indispensable to define the goals to be achieved, such as what type of services will be provided and to whom. A crucial aspect of such a project is to find a dedicated sponsor, known in project management jargon as a senior figure.

This champion within the organization has ownership of the project, expects the project to succeed and works to ensure its complete realization. The role of sponsor is not merely an official one. Effective sponsorship is only possible if the sponsor is personally convinced of the project's value and is willing to champion it and support its staff at every formal or informal opportunity, throughout all stages of development.

It is imperative to have a clearly articulated vision of how the analytical unit will be developed to advocate for resources to the organization's senior management. High-quality analytical units are not a cheap endeavor, particularly the cost of analytical software, data collection and storage capabilities, and data acquisition as well as maintenance and other recurring fees. And of course, there are the people. Apart from salaries, there will be expenditures for regular training and education. Any project needs a manager responsible for coordination, but even more importantly, dedicated team members who understand the mission and not only support it, but continuously develop the internal processes and the analytical craft of the unit.

It is imperative to have a clearly articulated vision of how the analytical unit will be developed to advocate for resources to the organization's senior management.

Key Competencies

For an efficient analytical endeavor, two groups of staff should work closely together — analysts and a data team responsible for data collection and maintenance of analytical software. Each requires a specific skill set. Analysts need in-depth knowledge of national and international security issues. In some cases, they need regional expertise accompanied by a significant proficiency in multiple languages. They must understand the fundaments of the technical aspects of cyber security, as well as information security policies and processes. Other crucial elements of the job include proficiency in the craft of intelligence analysis, open-source intelligence (OSINT) tools and techniques, and a working knowledge of analytical software supported by the data team. The two most important roles on a data team are the data engineers, who have expertise in big data infrastructure management, and the data scientists, who have in-depth knowledge of data integration, information science and data visualization tools.

Regarding analytical positions, the current market is unlikely to provide candidates with the complete package of skills, making it necessary to compromise and identify key competencies that can be built upon. The following prerequisites are cornerstones for further professional development: boundless curiosity and enthusiasm for the subject; a willingness to constantly learn; the ability to grasp complex and evolving concepts; the ability to understand the implications of cyber issues in the physical world; excellent written and spoken presentation skills in the national language; fluency in English and in the case of regional experts, a decent knowledge of the regional language. From this base, other skills and knowledge can be added.

HEAD OF ANALYTICAL DEPARTMENT	
Analytical Unit • Regional security experts • Transnational security issues experts	**Data Unit** • Data engineers • Data scientists

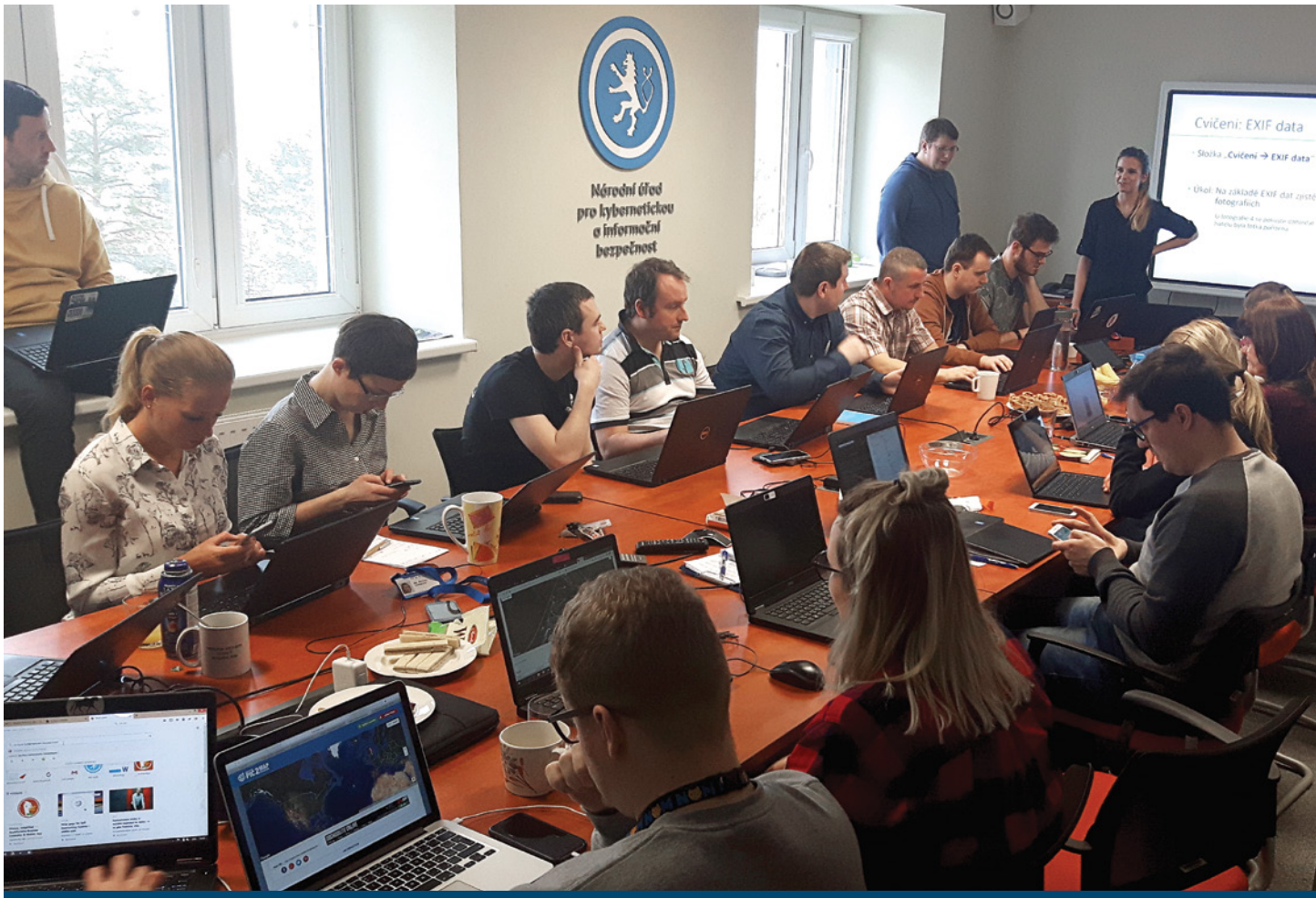
As a relatively small organization, NÚKIB extensively uses on-the-job training, as well as external training provided by institutions such as the NATO School Oberammergau, the NATO Cooperative Cyber Defence Centre of Excellence or private companies. Over the course of approximately three years, analysts undergo training in OSINT, analytical skills, cyber threat intelligence, specialized software and language courses. In that time, all analysts have sufficient opportunity to participate in dozens of analytical projects, support the handling and investigation of critical incidents, and create personal networks for interagency cooperation. After a sufficient period, promotion to senior analyst can be considered.

Professional development in the field of cyber security is never-ending because anything learned in OSINT, cyber threat intelligence, analytical software, etc., more than two or three years ago risks being obsolete. To be up to speed on cyber security, international political development and several other major fields mentioned above requires true analytical superheroes.

After the initial training and general introduction to the job, there is a new challenge: how to motivate the analysts and prevent them from leaving. There is no simple solution, though keeping analysts involved in the major issues of the day and letting them see firsthand the impacts of their work has proved effective at NÚKIB. Another long-term strategy is job rotation in cooperation with the agency's CERT and other horizontal opportunities for professional growth.

Technology Supports the Mission

People are the most critical asset, for which no technology can substitute. Keeping this in mind, the right technology helps to automate as many processes as possible so that analysts can focus on the activities with the highest added value and eliminate any repetitive undertakings. However, there are limits to the absorption of new technologies. Both data and analytical teams can handle only a finite number of software tools and make full beneficial use of them. Therefore, special care must be taken at the beginning of the planning process to choose



Cyber security analysts from the National Cyber and Information Security Agency's (NÚKIB) Strategic Information and Analysis Unit meet at NÚKIB's headquarters in Brno, Czech Republic. NATIONAL CYBER AND INFORMATION SECURITY AGENCY

technology that will best support the mission. It is especially important that the main pieces of analytical software be tools that will help the analysts, not overwhelm them. The data team will consist of people with technical education and data scientists. It is essential that they understand the mission of the unit and the needs of the analysts.

Talent Scouting and Outreach

Since its beginning, the NÚKIB analytical unit has conducted outreach activities to attract new talent to the unit and to the agency in general. Unlike some security agencies, NÚKIB can and must be visible. Outreach activities include lecturing at universities, security or cyber security programs of think tanks and other institutions, and presentations at conferences.

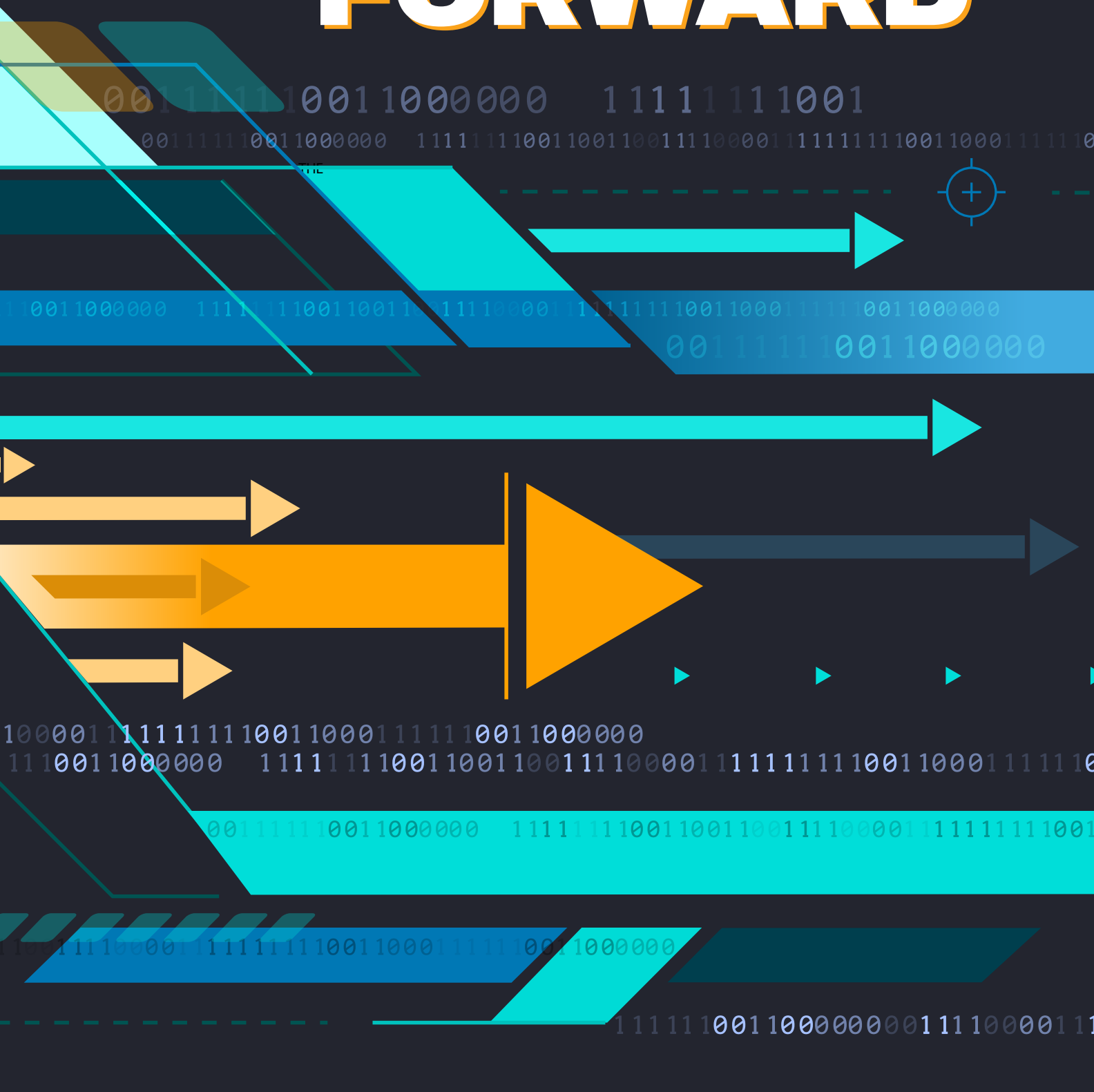
The unit collaborates with the security studies program at Masaryk University in Brno in the Czech Republic, which has generated a substantial pool of applicants for the internship program and jobs at NÚKIB. The internship program has proven to be an excellent introductory opportunity for students interested in careers in government institutions and a great way to practically test potential future co-workers.

Conclusion

Considering international developments and initiatives such as the European Union Toolbox on 5G Cybersecurity or the Prague Proposals, the importance of the nontechnical aspects of cyber security and contextualization of cyber threats will grow in coming years. If national-level institutions responsible for cyber security are to keep pace without depending on third-party expertise, they must establish the necessary analytical capabilities. NÚKIB has been developing this capability for more than four years to support the policy cycle and provide analysis of cyber security issues to top decision-makers in the government and other strategic institutions.

Establishing an analytical unit should be approached as a project requiring long-term dedication from the staff and organizational leadership. The analysts and data team are the most critical assets. Analytical job candidates possessing all the necessary skills are rare. They must be developed by identifying and building on key competencies. Maintaining development in both the technical and nontechnical aspects of cyber security requires true analytical superheroes. ◻

THE BEST PATH FORWARD



How to Effectively Develop a Regional Cyber Security Workforce

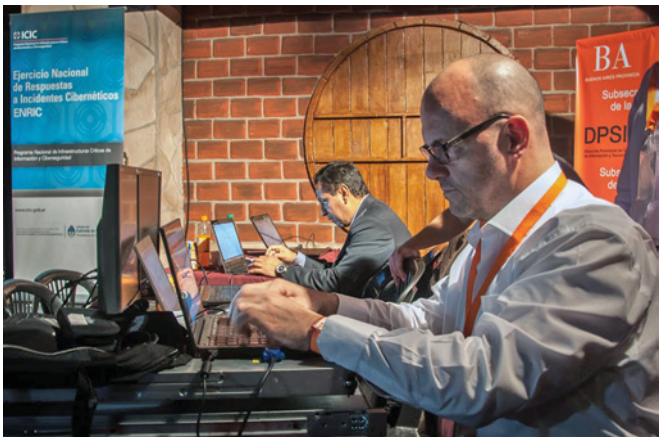
By **Pedro Janices**, academic coordinator for the CAPA 8 Foundation; **Mariana Galan**, legal advisor to the Directorate of Cybercrime of the Ministry of Security of Argentina and member of the Commission on Public Policies, Human Rights and Digital Privacy for the CAPA 8 Foundation; **Maximiliano Scarimbolo**, principal officer for the Buenos Aires City Police; and **Agustin Malpede**, lawyer specializing in information law at the University of Buenos Aires

PHOTOS BY NICOLAS LOPE DE BARRIOS

The outbreak of COVID-19 in early 2020 created an urgent need for some countries to adopt social isolation measures and to encourage teleworking, forcing companies and governments to use all the digital tools at their disposal and to increase their availability and access. Organizations that had little or no digital infrastructure were forced to acquire and deploy new digital resources in a very short time, learning as they went.

The pandemic has resulted in a state of increased hyperconnectivity. This is due to a number of factors, such as business and service continuity and an increase in leisure time and digital relationships, forcing people into information self-overloads and making apparent the need for multidisciplinary cyber security teams that focus on crime and safety.

The situation has also brought to light the importance of critical information infrastructure, showing that cyber security not only affects states and the private sector, but also everyone who maintains, contributes to and uses networks. This demonstrates the urgent need to work toward the development of a cyber security workforce that allows nations to take progressive action by training personnel, promoting cyber security awareness in society, passing necessary laws to build a solid legal framework and proposing new public policies in cyber security-related matters. This is not an easy task since it requires the collaboration of every actor involved, each in one's own place, to secure what is necessary to collaborate in the development of a cyber security workforce.



While some countries in Latin America and the Caribbean have shown interest and commitment to training and exercising to develop further capacities, much still needs to be done to consolidate an ecosystem among the various sectors that allows taking the necessary actions on a regional basis.

From a cultural and social point of view, the development of a regional cyber security workforce should include values, practices and attitudes, and the habits of individual users, experts and other actors in the cyber security ecosystem. The cultural and social perspective varies according to the roles and functions of the actors within this ecosystem. Economic factors also significantly influence whether cyber security measures are efficient.

Law enforcement agencies throughout the region are fully involved in the investigation of cross-border crimes, collaborating with their regional and international counterparts.

LAW ENFORCEMENT

In the field of law enforcement, officers receive constant training in cyber security, although most of them are explicitly focused on cyber crime and cyber terrorism. These activities involve both governmental and nongovernmental organizations (NGOs), which provide a wide range of instructors from Latin America and other regions of the world.

Law enforcement agencies throughout the region are fully involved in the investigation of cross-border crimes, collaborating with their regional and international counterparts. However, in a number of Latin American countries, due to their investigative systems, law enforcement agencies do not have the comprehensive institutional capacity required to investigate and handle cyber crime-related cases and other digital felonies. In these countries, this is the prerogative of the judiciary system, which often leads to bureaucratization and slow investigations.

Informal training, meetings and workshops have proven useful when promoting regional integration and cooperation among numerous agencies, helping to create nonofficial networks of contacts and cooperation channels. Law enforcement now needs to formalize these networks of contacts and links and advance to a more planned and professional system of training.

Law enforcement agencies must monitor and assist this progressive professionalization process wisely, creating technical and operative multiagency protocols and providing the necessary training at each level, which will raise standards and empower the cyber security workforce.

Significantly, establishing regional training and capacity building integration between law enforcement agencies would generate a solid workforce that can face the global challenges of cyberspace.

Argentina, for example, conducted the National Cyber Incident Response Exercise between 2011 and 2015, training a 30-member task force, integrated with members of federal law enforcement forces (Federal Police, Coast Guard, Gendarmerie and Airport Security Police), the Armed Forces, lawyers, prosecutors, judges, technical teams from companies and members of government agencies. These exercises, which began under the auspices of the Organization of American States (OAS) Inter-American Committee Against Terrorism, gave impetus to the need for joint work and the development of specific capacities respective of local laws and culture. Despite these constructive efforts, Argentina's change of government brought in an administration with a different philosophy regarding the exercises, which were discontinued in 2016.

Participants at the National Cyber Incident Response Exercise, May 14, 2015, Mar del Plata city, Buenos Aires, Argentina

PRIVATE SECTOR

Despite efforts being made, Latin America still finds itself in a situation of urgent need. According to the "Cybersecurity Report 2018-2019" from VU Labs, a company that focuses on fraud prevention and identity protection, 45.3% of participating organizations from different countries were victims of a cyber attack during the past three years. In the same vein, according to the "2018 Internet Security Threat Report" by Symantec, Argentina occupies eighth place as the country of origin for cyber attacks. Although the 2016 cyber security report from the OAS and the Inter-American Development Bank (IDB), "Cybersecurity: Are We Ready in Latin America and the Caribbean?" indicates that the region is accelerating development in cyber security matters, regional capabilities are still limited compared to our European counterparts.

In Latin America, the local branches of multinational corporations do not strive to raise cyber security awareness, as do their head offices. As a result, they fail to develop an adequate cyber security workforce that allows them to face the many challenges that cyberspace presents. Here, the academic sector will play a fundamental role. At this time, cyber security-related topics can only (and hardly) be found in university careers or postgraduate courses, severely limiting the possibilities for developing a strong, cyber-resilient and cyber-aware workforce.

To overcome these obstacles, Latin American countries need to set clear and transparent rules and lay the foundation for a solid legal framework, taking actions such as:

- Supporting and developing national cyber industries that are best suited to understanding local culture and identifying the cyber security needs of each country in the region. This is done, for example, by creating effective tax incentives for actors who invest in and promote the evolution of information and communication technologies (ICT).
- Strengthening public-private cooperation involving national and international ICT companies, as well as the academic sector and civil society. This would close the gap between sectors and generate a wide, integral vision of the current state in the region.
- Developing societal trust in national digital infrastructure, promoting collaboration in every sector and allowing each citizen to be involved in the decision-making process.
- Enhancing traditional education tools at every academic level, helping citizens to adopt new habits with full knowledge of the risks that cyberspace represents.

Raising the maturity level of subsidiaries of multinational companies in the region will allow, among other benefits, the adoption of safety standards for this sector, the defining of security policies and the implementation of new methodologies. It will raise awareness of the security risks and the training of human resources from a security point of view, generating opportunities to share knowledge and experiences. The private sector must understand the need to use standards developed specifically to deal with cyber security-related matters and comply with the necessary legal framework accompanying the process.

PUBLIC SECTOR

The region's public sector awareness of the importance of developing cyber security strategies and regulatory frameworks has increased in recent years, reaching a medium level of commitment as indicated by the "Global Cybersecurity Index 2018" from the United Nations' International Telecommunications Union.

While some Latin American countries are in the process of developing their own strategies, others, such as Argentina, Chile, Colombia,

National Cyber Incident Response Exercise, May 20, 2014, Puerto de Buenos Aires, Argentina

Mexico, Paraguay and Peru, already have theirs in play. This fundamental pillar must be considered when trying to generate long-term public policies and regulatory frameworks. The maturity level of these strategies varies, including in terms of providing a framework for cooperation between government agencies, critical infrastructure operators and the private sector.

Latin American countries have different approaches, priorities and attitudes regarding the development of a cyber security workforce. While the public sector recognizes the need to work on topics that range from internet governance and innovation, to providing public services and the acquisition of digital equipment, there is still a medium/low level (50% average) for internet penetration in the region.

Social and economic problems play major roles in defining each country's vision regarding the development of its workforce. For example, some will have a more privacy-oriented vision and others may choose a military approach to the subject.

The development of a solid legal framework, new standards and technical regulations is moving slowly in the region. As mentioned before, only a few Latin American countries have implemented their own cyber security strategies and even fewer consider it a necessary state policy, update their digital infrastructure or focus on capacity building.

International organizations such as the OAS or the IDB provide constant support in raising cyber security awareness and capacity building. They also encourage countries to join different international initiatives such as the Global Forum on Cyber Expertise and the Internet Governance Forum.

Some Latin American citizens don't fully understand the risks and vulnerabilities that ICTs present. This has led countries from the region to make efforts toward sensitizing and training human resources, which will continue over time, and even to associate with international campaigns, aiming for a cyber-resilient and cyber-aware society.

In the case of a cyber incident, the amount of information passed through formal channels is rather low. On the other hand, much more information flows through informal channels. Formal channels seem to be severely affected by factors such as the fear of filing a formal complaint, poor complaint communication mechanisms and by the lack of knowledgeable authorities to receive them, and even by the difficulty of taking not only reactive, but preventive measures.

This is closely linked to the adoption of regulatory frameworks to prevent cyber crime. Most countries in the region understand the transnational nature of these crimes, and cooperation has deepened in recent years. Argentina, Chile, Colombia, Costa Rica, the Dominican Republic, Panama, Paraguay and Peru have now acceded to the international Budapest Convention, a treaty that addresses cyber crime. Work is also under way in a number of intergovernmental bodies on the drafting of new instruments of cooperation in which a larger and more diverse group of countries can discuss criminal conduct and new cooperation mechanisms with an understanding of regional asymmetries. However, the prosecution rate of cases is low, the judiciary does not have sufficient forensic tools for investigations, and training in this area is scarce.

NGOS AND CIVIL SOCIETY

NGOs play a major role in Latin America, especially in Argentina. They contribute to and cooperate in visualizing, understanding and even improving public policymaking. This is why it is vital to take into consideration the opinion of every actor involved and promote the development of a solid legal framework that focuses on privacy, human rights, and capacity building of technical and legal resources.

NGOs are also an important source for free debate, speech and thought, which will considerably benefit the strength and resilience of regulations applied in each state. Accordingly, a United Nations resolution (A/RES/73/27), passed on December 5, 2018, endorses this type of government support: "States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behavior in information space with regard to their potential role."

Clear examples of this are the workshops and congresses where Fundación CAPA 8, an Argentina-based nonprofit that studies and advocates for cyber initiatives from a human rights perspective, gathered representatives from the executive, legislative and judicial powers, as well as law enforcement and the armed forces. The private sector, academy and press were also present and contributed with their knowledge and viewpoints, generating a healthy debate about the successes, errors and challenges that Argentina faces in its fight against cyber crime.

CONCLUSION

The Global Information Security Workforce study, conducted by the Center for Cybersecurity and Education in 2017 in 170 countries, reveals that there will be a cyber security manpower shortage of more than 1.8 million workers by 2022 and concluded that there are not enough cyber security workers in organizations to address the challenges they face today.

Workforces that focus on protecting a country's cyberspace require expertise and both initial and continuing professional training to be able to respond adequately to the scale and evolution of cyber incidents. Generating the necessary training from the law enforcement training institutes (Federal Police, Coast Guard, Gendarmerie and Airport Security Police) would require at least two years of instruction.

For this, it is necessary to promote state policies on cyber issues, sustained over time through the essential contributions of the different actors in the cyber ecosystem: the public and private sectors, academia and NGOs.

The "new normal" will find us with hyper-connected governments, companies and citizens, and we will have to respond to threats with specialized technical, legal and diplomatic teams.

Cooperation and collaboration between countries ceases to be mere diplomacy and becomes a case of cyber survival for all and working toward regional resilience. To this date, progress in Latin America, in most cases, has been the result of efforts that have also highlighted the weaknesses of those countries in the region that have not yet begun the journey.

The "new normal" will find us with hyper-connected governments, companies and citizens, and we will have to respond to threats with specialized technical, legal and diplomatic teams. Will we be on time? Will we come to equalize the regional asymmetries? The challenge is ours. ◻

A COLLABORATIVE APPROACH

Serbia's Cyber Security Education, Training and Workforce Development Strategy

By **Jelica Vujadinović** and **Dr. Marko Krstić**
Serbian National Computer Emergency Response Team

The Serbian government's significant digitalization efforts have resulted in increased efficiency and more transparency in its public services but have also exposed the country to cyber attacks. Addressing this problem inadequately could degrade the public's well-being by destroying economic gains and disrupting the services crucial to everyday operations, such as electricity production and delivery.

Since formal education in the field of cyber security is still emerging — with a few master's programs currently available — the government identified this gap and appointed the Serbian National Computer Emergency Response Team (SRB-CERT) as the authority to develop nonformal education for critical infrastructure operators. SRB-CERT has some experience in providing education; one of its members helped design a cyber security course and is now an information-technology industry lecturer for the course at Master 4.0 Advance Information Technology Applications in Digital Transformations, a program provided by a consortium of faculties.

Education Strategy

The strategy adopted by SRB-CERT combines two principles: Act promptly and be proactive about emerging threats. New amendments to the Law on Information Security were adopted in 2019, instructing the Ministry of Trade, Tourism and Telecommunications to create a list of critical infrastructure operators. Even before the ministry created the list, SRB-CERT began to provide training to local governments, which are the stakeholders with the least specific information and communications technology infrastructure. Communication and cooperation with local governments were facilitated by the National Alliance for Local Economic Development. Cooperation and information sharing were further enhanced through a public-private partnership with Microsoft, which was selected because it is the principal vendor of operating systems for local governments.

Artificial intelligence (AI) had been recognized as the emerging technology that could most significantly increase the benefits of digitalization, but it also introduces new attack vectors. To prepare for future e-government challenges, SRB-CERT started examining the implications of AI for the threat landscape. At the time, the working group formed by the government was drafting the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for 2020-2025, and it was vital for them to consider the AI security aspect. It was good timing for the SRB-CERT team to present results of their research on the potential impact of AI on cyber security at the 2019 International Telecommunications Forum in Belgrade.

Educating Local Governments

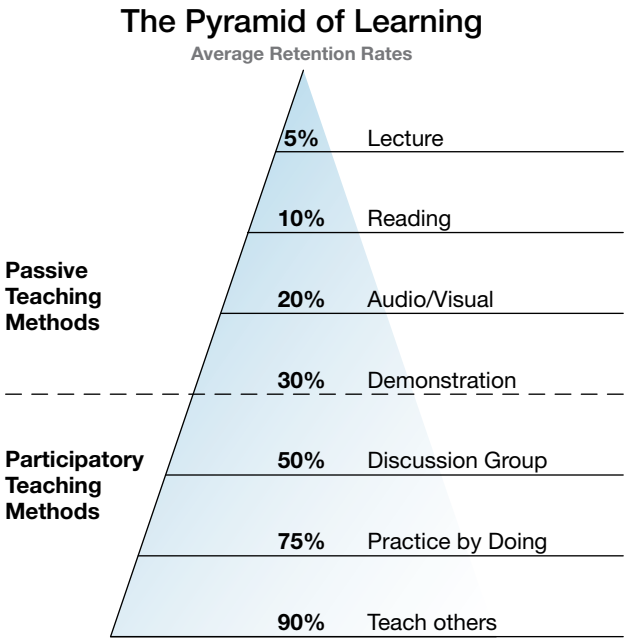
Training for local governments consisted of a legal component, intended for managers and technical staff, and a technical component for system administrators.

The legal component was organized to consider theoretical and practical aspects. Participants had the opportunity to find out more about a Confidentiality-Integrity-Availability concept, active threats, cyber security incidents, security measures, a Plan-Do-Check-Act model and to get familiar with the Law on Information Security. The practical part focused on the Cybersecurity Act model, developed by SRB-CERT to support critical infrastructure operators in delivering this document, which is mandatory for their organizations under the legislation. During the training, the participants had the opportunity to write a procedure to address one of the 28 security measures adopted by the Law on Information Security from the ISO/IEC (a joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission) 27000 family of standards and described in the Cybersecurity Act model.

System administrators from local governments learned about common attacks in a Windows environment, authentication protocols, credential theft opportunities and the systematic defense approach proposed by Microsoft's experts through a series of theoretical presentations and practical exercises on the Cyber Attacks Simulation System, which was specially developed for this purpose.

Concepts of training were selected to combine the passive and active teaching methods of the pyramid of learning. The participants could attend lectures, read, access audio and visual content, observe demonstrations and participate in discussions and practical work. Furthermore, because SRB-CERT members rotated as trainers, they all benefited from the role of educator, which gave them a chance to improve their knowledge.

Participants listen to a panel at a seminar for local governments in Kragujevac in October 2019. SRB-CERT



Source: Adapted from the National Training Laboratories, Bethel, Maine, U.S.

Special attention was paid to standardization, in line with Global Forum on Cyber Expertise efforts to adapt and adopt the National Initiative for Cybersecurity Education (NICE) Workforce Framework in Europe. The technical component combined the important knowledge, skills and abilities (KSAs) from the system administrator, cyber defense analyst, system security analyst, cyber defense incident responder and vulnerability assessment analyst roles. This resulted in the following KSAs, which describe the competencies developed through the training:

Knowledge of:

- Cyber security and privacy principles.
- Cyber threats and vulnerabilities.
- Specific operational impacts of cyber security lapses.
- Organizational information technology user security policies.
- System administration, network and operating system hardening techniques.
- Application vulnerabilities.
- Cryptologic capabilities, limitations and contributions to cyber operations.
- Current software and methodologies for an active defense and system hardening.
- Methods and techniques used to detect various exploitation activities.

Skills in:

- Maintaining directory services.
- Extracting information from packet captures.
- Verifying the integrity of all files.

Abilities to:

- Apply cyber security and privacy principles to organizational requirements.
- Monitor system operations and react to events in response to triggers and/or observed trends or unusual activity.

Nearly 200 participants from 79 local governments have attended training by SRB-CERT. The training was made available in every region of Serbia: the Central and Western region, the Southern and Eastern region, the Northern region and the Belgrade region. After each session, the participants were interviewed to measure their satisfaction and to identify room for improvement.

Future Threats From AI

Future threats from AI were analyzed using possible applications of machine learning (ML) in CERT operations. This topic was selected for three reasons:

- To inform the academic audience about the jobs and tasks of the cyber security workforce in a CERT team.
- To describe how ML could increase the efficiency of CERT operations.
- To raise awareness about the security aspects of AI.

Even though the focus remains on the development of specialized training, the presentation revealed important facts for further workforce development. The potential of ML for CERT services became evident, including security-related information dissemination, incident handling, malware analysis and cyber exercises. However, using this technology comes with a risk. Although the National Institute for Standards and Technology is still working on the ML attack taxonomy, not all attacks are equally probable, nor do they lead to the same consequences. This means that models of attackers' realistic capabilities need to be considered during threat analysis, and the secure software development life cycle must include vulnerability scanning and model hardening.

Even though, so far, the current version of the NICE framework recognizes ML theory and principles only as an important aspect of the data analyst role, it has a much greater potential to transform many other work roles as well.

The positive impact of the presentation cannot be overstated, and the Strategy for the Development of Artificial Intelligence, which was adopted several months later, addressed the security aspects accordingly.

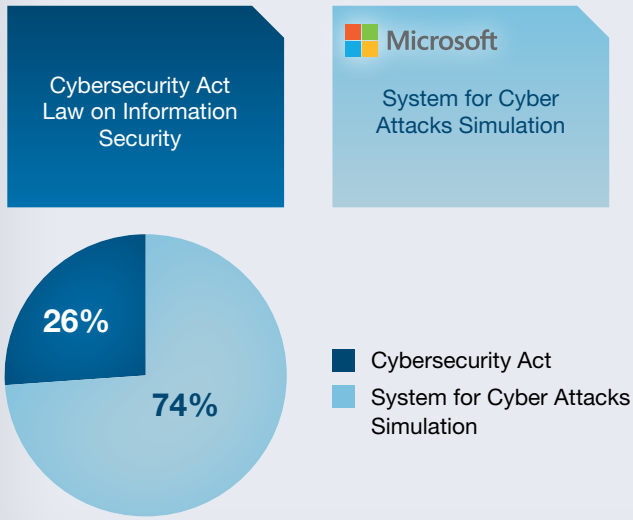
Conclusion

Serbia is the only country in Southeast Europe that has adopted the standardization approach in designing training and establishing a Strategy for the Development of Artificial Intelligence, offering a unique opportunity for other countries to learn from Serbia's experience and results.

The training for local governments provided by SRB-CERT resulted in increased trust, enhanced cyber awareness and improved knowledge, leading to an increased number of incidents reported by local governments. This process also made it possible to identify improvements for

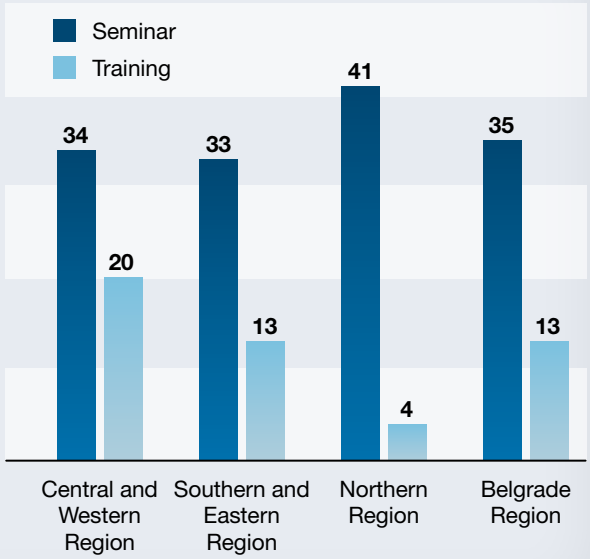
The Djerdap I hydroelectric power station near Kladovo, Serbia, is the largest dam on the Danube River. Protecting critical infrastructure from cyber threats is a growing challenge. AFP/GETTY IMAGES

Seminars | Technical Trainings



Source: Adapted from the National Training Laboratories, Bethel, Maine, U.S.

Participants Per Region



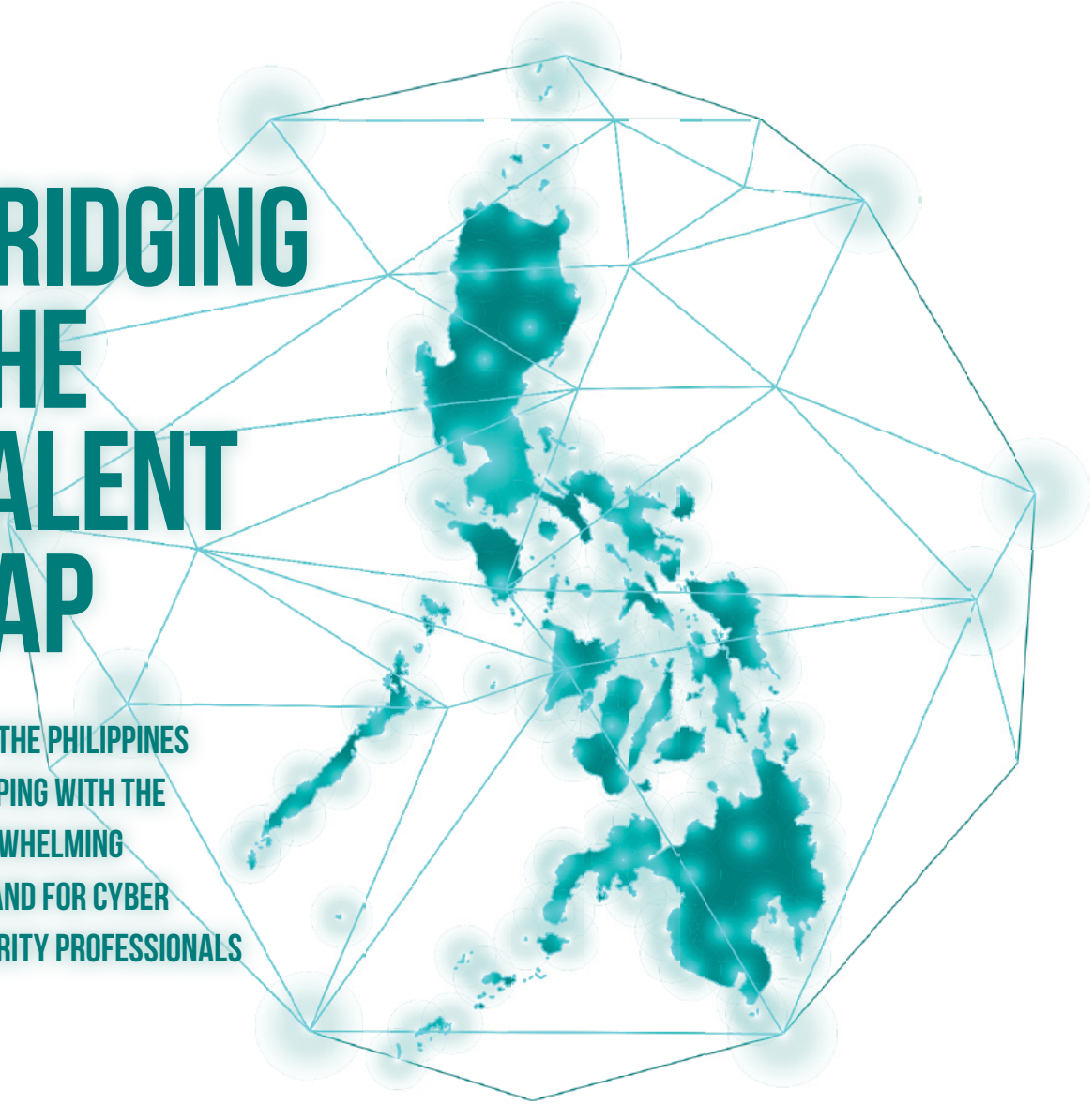
Source: SRB-CERT

subsequent training. The knowledge, skills and abilities of the SRB-CERT members have been significantly improved, and it has been confirmed that the Cybersecurity Act model developed by SRB-CERT can be applied and easily adjusted to any of the participant organizations. Although the results of the training standardization cannot be detected in this short period, it is expected that more accurate information about work roles and training requirements will be available in a future phase. The focus of future training will be on the development of advanced education for local governments and, by following the same methodology, on a basic level of instruction for other operators of critical infrastructure.

The first steps in making AI-related security training have already been taken. Further research is needed to fully define the syllabus, the target audience and learning methods. A recent study by the Future of Humanity Institute at Oxford University in the United Kingdom showed that scientific research on AI offense-defense balance is different from research on computer security because there is a much greater probability of revealing methods that adversaries would not discover by themselves but are capable of exploiting for attacks. It is, therefore, recommended to discuss offensive aspects together with defensive solutions and to avoid providing information about attacks that contain not-so-easily-patched social components, whereas special precaution should be taken in situations when source codes are shared. ◻

BRIDGING THE TALENT GAP

HOW THE PHILIPPINES IS COPING WITH THE OVERWHELMING DEMAND FOR CYBER SECURITY PROFESSIONALS



By **Genalyn B. Macalinao**, information technology officer, Philippine Department of Information and Communications Technology

Lockdowns around the world have placed economies at a standstill, slowing the virus's spread but causing a heavy economic toll. In the Philippines, an overwhelming majority of companies are encouraging or requiring their employees to work from home because of COVID-19, so it's no surprise that cyber security and data privacy issues have started to surface.

Never before has the country's lack of cyber security professionals been more glaring. While the issue has been brought up several times by cyber security stakeholders, it is in this national emergency that everyone in the country felt the dire need for a strong cyber security infrastructure and a workforce capable of ensuring continued operations of the government and other critical infrastructure.

Workers across the information technology (IT) sector are needed more than ever to enable governments and critical infrastructure, help businesses stay online and keep citizens connected. Cyber security professionals are critical to supporting health care providers, manufacturing technology products and components, securing and servicing critical data centers, delivering food and essential needs to communities, keeping out-of-school students engaged, and enabling governments to respond to this global health crisis.

At a time when their skills are essential, there's a major gap between the number of qualified cyber security workers and what is needed. Even before the onset of the pandemic, Cybersecurity Ventures projected that the shortage would spark an industry crisis with a staggering 3.5 million unfilled positions by 2021. In 2016, the Philippines trailed its peers in the Association of Southeast Asian Nations with only 84 Certified Information Security Systems Professionals (CISSP), according to (ISC)[2]. Indonesia had 107, Thailand had 189, Malaysia had 275, and Singapore had 1,000. On top of this, half of the 84 Filipino CISSPs were reported to be working overseas. A study conducted by IBM and the Ponemon Institute in 2018 showed the cyber security talent deficit carries immense risks as the number of sophisticated data breaches increases without competent professionals to

detect and prevent attacks. Testament to that are a number of high-profile cyber security incidents and data breaches that have plagued the Philippines one after another.

A prime example is the data breach of the Commission on Elections. On March 27, 2016, hackers under the banner "Anonymous Philippines" hacked into the website of the Philippine Commission on Elections and defaced it. The hackers left a message calling for tighter security measures on the vote-counting machines to be used during the May 9, 2016, Philippine general election. Without a cyber security plan in place, the country was left at the mercy of cyber criminals.

A month after the elections, the law creating the Department of Information and Communications Technology (DICT), Republic Act No. 10844, was signed.

- The protection for supply chains through a national common criteria evaluation and certification program.
- The protection of individuals through the acceleration of learning skills and development, a cyber security outreach project, a national cyber security awareness month, and equipping the government and the program for local and international cooperation.

The Cybersecurity Bureau of the DICT conducts roundtables with the 12 CII sectors (government, information communications, energy, aviation, maritime, land transport, health care, banking and finance, water, security and emergency, media, and business process outsourcing), inviting the academe for awareness on industry needs. It is this endeavor

To further engage Philippine youth in cyber resiliency initiatives, the Department of Information and Communications Technology coordinates with the Department of Education to integrate cyber security curriculum in senior high schools.

Eliseo Rio Jr., left, then acting secretary of the Department of Information and Communications Technology, and Felizardo Colambo, president of AMA Computer University Inc., sign an agreement in 2019 meant to increase the number of cyber security professionals.

PHILIPPINE DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

The DICT is a government agency tasked to develop policies and plans for information and communications technology (ICT) development in the country. It exercises broad powers over telecommunications and broadcasting, cyber security, data privacy, consumer protection, and the promotion of trade and investment in ICT and ICT-enabled services. The department was barely a year old when it launched and published the National Cybersecurity Plan (NCSP) 2022, a five-year plan that serves as the country's road map to its vision of a cyber-resilient Philippines.

The NCSP provides the foundation for cyber security policy-making, covering the implementation plan. Key strategic initiatives were laid out, featuring a holistic and multilayered response system to better protect critical infrastructure against cyber threats. A key imperative of the National Cybersecurity Plan is to support the development of cyber security professionals.

The NCSP 2022 sets out the following key program areas to address the need for increased awareness and capacity building for the public and private sectors:

- The protection of critical information infrastructure (CII) through cyber security assessment and compliance, national cyber drills and exercises, and a national database for monitoring and reporting.
- The protection of government networks through a national computer emergency response program, a capacity building and capability development program, a pool of information security and cyber security experts, the Threat Intelligence and Analysis Operations Center, protection of electronic government transactions, and the update of licensed software.

that paved the way for partnerships with the academe in the development of cyber security curricula.

The bureau also sits on the technical panel of the Commission on Higher Education (CHED) for the development of policies, standards and guidelines (PSG) for the bachelor's program in cyber security. The PSG is now in its second draft and is currently in the consultation phase.

While waiting for the release of CHED's PSG for the Bachelor of Science in cyber security, the DICT is continuously appealing to schools to integrate cyber security into their curricula.

Some institutions now offer new cyber security courses. This is part of the Philippines' efforts to strengthen students' skills in science, technology, engineering and mathematics (STEM). As the first IT school in the Philippines, it is no surprise that AMA University is the first school in the country to offer a bachelor's degree in cyber security. This was realized through a partnership with the DICT Cybersecurity Bureau and inspired by the cyber security curriculum developed by the George C. Marshall European Center for Security Studies. In response to the need for formally educated cyber security professionals, AMA University is now accepting enrollees at its main campus in Quezon City, Philippines. An initiative from the private sector is the partnership between the security firm Palo Alto Networks and Asia Pacific College to launch the first cyber security academy in the Philippines.

While some schools in the Philippines have integrated cyber security into their curriculum, much still must be done to bridge the huge gap between industry needs and a cyber security workforce with the right skills. ◻

DEFENDING MAURITIUS
AGAINST CYBER THREATS

The nation's G-SIRT fights the never-ending battle to build cyber defense capacity

By **Madan Kumar Moolhye**, Information Technology Security Unit, Mauritius Ministry of Information Technology, Communication and Innovation

The last three iterations of the Global Cybersecurity Index (GCI) published by the United Nations' International Telecommunication Union have ranked Mauritius as the country most committed to cyber security preparedness in Africa. How the Government Security Incident Response Team (G-SIRT) approaches capacity building — one of five pillars of criteria evaluated in the GCI — is evaluated here.

Importance of Capacity Building

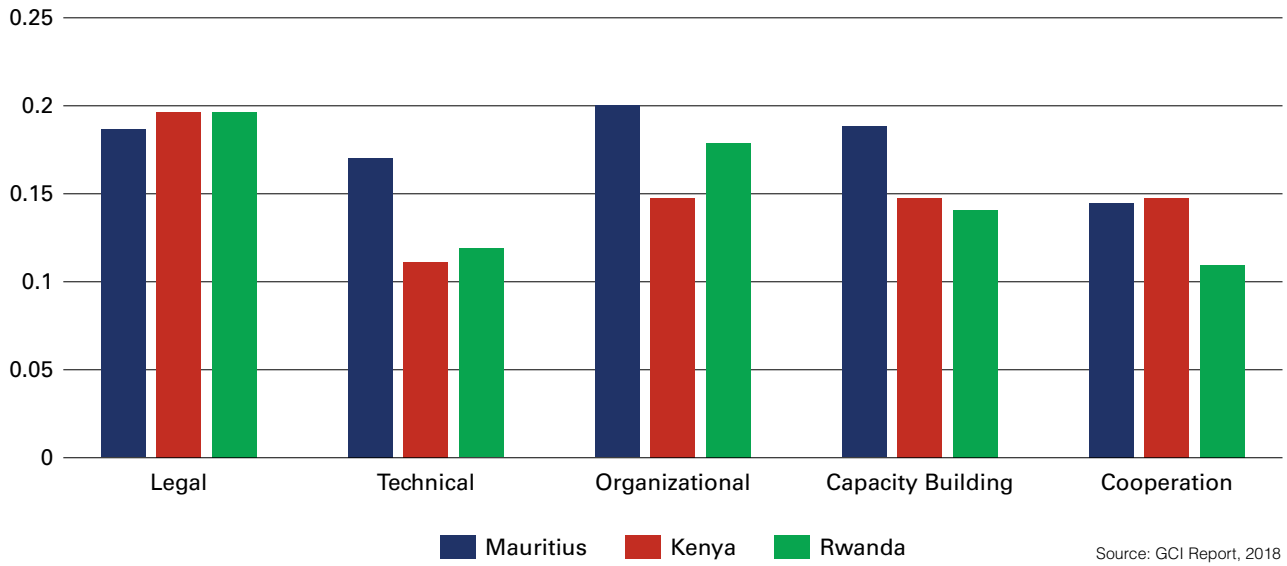
The G-SIRT operates under the Information Technology Security Unit (ITSU) of the Ministry of Information Technology, Communication and Innovation. The ITSU emphasizes the importance of constant development of its technical staff to achieve its objectives, which are:

- Implementing government policies regarding information technology (IT) security.
- Assisting ministries/departments in implementing security standards.
- Disseminating information on IT security.
- Carrying out security audits.
- Handling IT security incidents.

Cyber security awareness is accessible to a wide range of public officers through various deployment modes, such as:

- IT security awareness presentations conducted on-site.
- Circulation of fact sheets on security threats such as phishing, ransomware and identity theft.
- A cyber security module available via a 24/7 electronic learning system.

Top three scores in the Africa region according to the five pillars of GCI



Source: GCI Report, 2018

IDENTITY THEFT

'Know the Dangers'

What is Identity Theft?
Identity theft happens when an imposter uses someone's personal information such as name, address, identity number, credit card or bank account numbers for fraudulent purposes. This may also apply to an organization where a fake profile is created. Identity theft is considered as one of the most common cyber crimes in the world.

Fraudsters can get one's personal information by:
- Using the internet to search about someone or an organization.
- Stealing someone's wallet.
- Stealing postal mail.
- Going through your garbage bin (dumpster diving).
- Making use of malicious software/forged emails.
- Stealing digital information.

If you suspect you are a victim of identity theft, contact the relevant authorities, such as the police or your bank.

Signs of Identity Theft
- Your account statements show purchases that you are not aware of.
- You receive credit cards for which you did not apply.
- You are denied credit for no apparent reason.
- You get calls or letters from businesses about goods/services you did not buy.
- You discover an online profile corresponding to your name/organization which you cannot access.

Consequences of Identity Theft
Once your information is stolen, it may be used to:
- Buy things using your credit card/bank account.
- Commit fraud in your name.
- Create fake profiles in your name.
- Put your own/organization's reputation at stake.

Protecting Against Identity Theft
- Do not give out your personal information, especially via electronic means unless you know who you are dealing with.
- Do not share your sensitive information (such as password, PIN number) with anyone.
- Use strong passwords for all your accounts.
- Shop on secure and trusted websites ("https").
- Never store personal information on computers in public places such as cyber cafes.
- Install an up-to-date antivirus/spyware software.
- Do not use the same password for different accounts.
- Exercise caution on social networking sites.
- Practice safe internet surfing.

Source: Mauritius Ministry of Information Technology, Communication and Innovation

The G-SIRT collaborates regularly with the national Community Emergency Response Team of Mauritius (CERTMU), which addresses incident response at the national level. The G-SIRT acts as a sectoral incident response team within government. The CERTMU has organized several training events and cyber security drill exercises for the public and private sectors at regional and international levels.

The last cyber training drill involved local government teams such as G-SIRT, the data center and IT operators from ministries and law enforcement agencies. One of the main training objectives was to empower the G-SIRT to run cyber drills for government officials in the primary sectors, such as health, energy and utilities, which is a major goal for 2020-2021.

Information Security Management

Adopting the International Organization for Standardization's (ISO) international information security standard (ISO/IEC 27001) in the public and private sectors was a key project in the National Cyber Security Strategy (NCSS) of Mauritius. For the public sector, a novel approach was devised by the ITSU to develop a centralized information security management framework, based on a risk management approach and aligned to the standard. The framework is composed of template risk-treatment plans, addressing security threats to processes that are common to all ministries and that can easily be customized to cater to each sector.

Technical officers have been trained in developing the framework, empowering them to act as the main facilitators to ministries regarding training and implementation. In addition, customized capacity-building, cyber security professionals of the ministry have been trained on default ISO standards curriculum by international certifying bodies, such as India's Standardisation Testing and Quality Certification Directorate. G-SIRT staff also have been trained as security auditors for internal audits.

Government Security Incident Response

The G-SIRT responds effectively to information and communications technology (ICT) security incidents by providing proactive and reactive services to combat cyber threats. As part of its reactive services, the G-SIRT oversees incident management in the civil service through an automated incident handling system that includes a knowledge database available to cyber security professionals and ICT operational staff. This web-based system allows automatic incident escalation — as compared to the previous manual method — which facilitates speedier incident management with wider knowledge sharing. The G-SIRT team has also provided incident training to the operational IT teams posted in the ministries/departments.

Technical staff participation in workshops and cyber drills helps improve incident handling and enhances the provision of security recommendations to the public

sector. Interactions during regional/international workshops facilitate learning and information sharing, which is of high importance because cyber threats know no boundaries.

Security incidents suspected to be cyber crime are referred to the Police Cybercrime Unit for investigation, as per the Computer Misuse and Cybercrime Act. The G-SIRT also interacts with the national CERT for incidents having national impact.

On the proactive front, the team conducts security audits across the entire civil service. However, given the increasing complexity of cyber threats, additional tools and relevant training will be required to effectively protect the government. Furthermore, the G-SIRT is contemplating increasing its range of services to include malware analysis and forensics, capabilities that will require additional capacity building.

Training and Certification

The main challenges faced by G-SIRT are continuous workforce development and certification of its staff to counter the continuous emergence of new cyber security threats. Although technical officers benefit from workshops and seminars offered by donor countries, the skills gap is widening with the advent of technologies such as artificial intelligence and the internet of things.

The proportion of certified officers is low compared to threats in new domains. Certified cyber security training is needed so the team is better equipped to handle threats. Furthermore, to deliver the proposed additional services (e.g., malware analysis, cyber security audits), capacity building must be increased.

Another NCSS project is the incorporation of cyber security in the educational curriculum at primary, secondary and tertiary levels. There is no question that having a cyber security-conscious population would assist in building capacity while developing future professionals for a cyber security industry. The G-SIRT can work with academia and provide industry expertise to young professionals to complement their learning.

Conclusion

The G-SIRT will continue to emphasize professional development as it considers expanding its range of services to combat cyber threats, thereby increasing its contribution to Mauritius' strong GCI ranking. To manage increasing cyber risks, a capacity-building program is essential to counter existing threats, as well as being sufficiently adaptable to handle threats from new technologies. ◻

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

'Know the RISKS to SECURE better'

Information Security

Information is one of the most valuable assets of an organization and exists in many forms. Information security refers to the protection of information from a wide range of threats so as to preserve its confidentiality, integrity and availability.

Information Security Management System

An ISMS is a management framework, based on a risk management approach, to implement and improve information security. It allows an organization to:

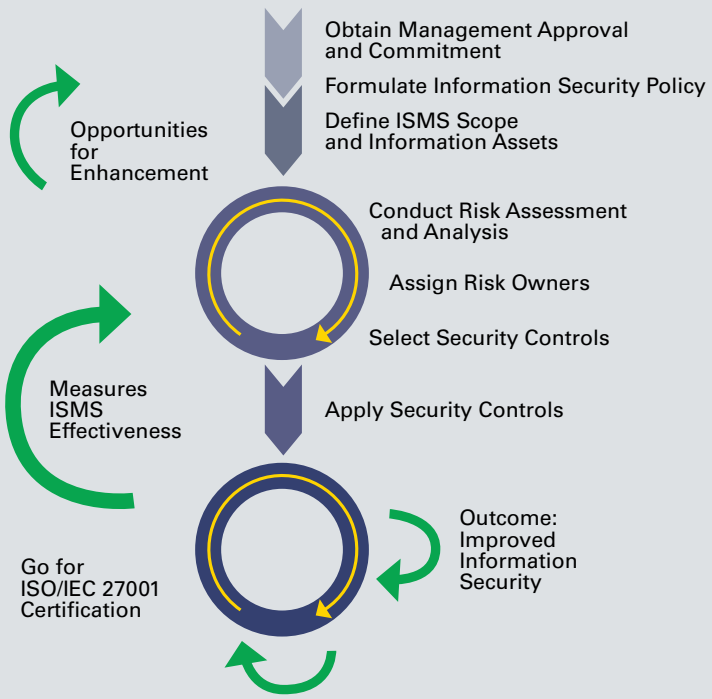
- Identify potential threats and their impacts on business processes.
- Evaluate the degree of risk in several areas.
- Apply adequate measures for eliminating or minimizing those risks.

The international standard ISO/IEC 27001 offers a comprehensive set of measures comprising best practices in information security, risk management and security controls.

Benefits of an ISMS

- Provision of user awareness on security threats and measures.
- Planning of effective business security objectives.
- Promotion of effective risk management.
- Better management of information security incidents.
- Increase in stakeholder confidence.

Steps to implement an ISMS based on ISO/IEC 27001



Source: Mauritius Ministry of Information Technology, Communication and Innovation

PERFECT SYMBIOSIS

CYBER SECURITY EXERCISES AND NATIONAL POLICIES

By **Veronika Netolická** and **Petr Novotný**, National Cyber and Information Security Agency of the Czech Republic

Cyber security exercises are perceived as one of the best tools for enhancing cyber security in the Czech Republic. They enable realistic crisis simulation in a controlled environment — and is there a better way to train/prepare for such a situation than to experience one? There are many useful and necessary tools (e.g., workshops, courses and conferences), but none can provide such a realistic opportunity as a cyber security exercise.

Like a Swiss Army knife, the exercises can be used for multiple purposes (see Figure 1). Such ability further underscores their effectiveness.

The ability to reveal and highlight blind spots in national policies can be achieved by various types of exercises — including technical, tabletops, procedural and communications exercises. Some are designed to check and assess national policies, while others might achieve that as a side effect.

Why assess policies by staging exercises? First, some policies may be obsolete. National policies and procedures might have been adopted long before critical systems became exposed to cyberspace. A good example is legal prescriptions for a state of emergency. These may have been in place for decades, but will they be of any use during a crisis in cyberspace? Second, assuming there is an up-to-date policy for active defense measures, how do you make sure it will be effective and applicable during an attack against critical infrastructure? It would surely be preferable to know before a crisis occurs. Finally, cyber security is a dynamic, quickly evolving field.

Policies need continuous updating, and the demand for new policies is ubiquitous. Consider the rollout of 5G networks: The next-generation of telecommunication networks represents a prime example of new technology that might create a need for novel national policies. Exercises have the ability to help reveal such demands.

When it comes to exercises, we apply a complex approach. Participants are invited from across all levels (strategic, operational and tactical), and all relevant aspects are covered (technical, political, economic, media, legal, ethical, etc.). Cyber security has been far more than a technical issue for the last couple of decades, spilling into other dimensions that include politics, the military, economics, legal issues and the media. These are all relevant to national policies. If these dimensions are covered in the exercise, appropriate participants must be present — legal experts, media experts, military officers and, especially, the decision-makers. In addition, it is a good idea to reflect new and upcoming trends in exercise scenarios. This helps to make them an effective tool in tackling emerging challenges.

Figure 1

MAPPING VARIOUS APPROACHES	IDENTIFYING BLIND SPOTS	REVISING POLICIES AND PROCESSES
IMPARTING KNOWLEDGE	PROVIDING INPUT ELSEWHERE	MAPPING THE STATE OF CYBER SECURITY
IDENTIFYING TRENDS	PROMOTING FOREIGN POLICY	SHARING EXPERIENCES

Source: National Cyber and Information Security Agency of the Czech Republic

Cyber security exercises are perceived as one of the best tools for enhancing cyber security in the Czech Republic. They enable realistic crisis simulation in a controlled environment – and is there a better way to train/prepare for such a situation than to experience one?

Synergy of exercises and national policies

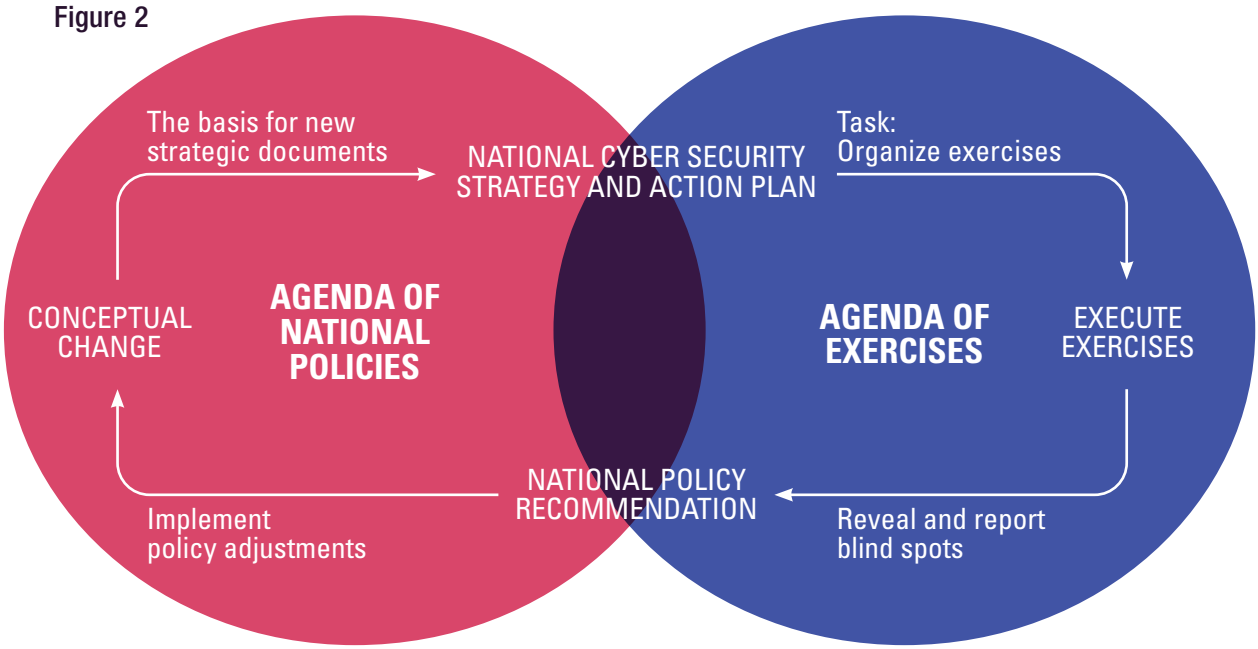
As shown above, revealing blind spots early is beneficial for drafting and adjusting effective national policies. Every exercise should aim to reflect the latest development with a focus on preparedness, which is closely related to a well-established and coordinated system. When a deficiency is detected, it is evaluated from the standpoint of the functionality of the national cyber security system. Based on the Czech experience, the process of identifying these spots in exercises is a closed circle of inputs and outputs. Inputs come from multiple sources — for example, previous exercises or their designers. However, the prime input contributors are national policy specialists. All of this input makes exercises sophisticated and more realistic. Output from the exercises should be relevant to national policy issues to be considered on an appropriate and strategic level. This process is based on people knowledgeable both in policy and in conducting exercises who can provide input suitable for the exercise and identify output fitting the purpose of national policy solutions.

The Czech experience and lessons learned

In 2016, the first document describing the blind spots in its national policies was introduced to the Czech government. The document was based on the Czech experience with the functioning of the system for ensuring national cyber security and contained analysis of the most fundamental problems that corresponded to the current framework. The outcomes of cyber security exercises are primary sources for this document. By processing these blind spots, it is possible to point out and focus on the primary lessons identified to make the process successful:

- **Workforce development** — People are a cornerstone of successful cooperation between the policy unit and exercise designers. Make sure they understand and appreciate each other's agendas and communicate regularly. The better input the policy unit can provide, the more valuable the outcomes will be. Allow national policy specialists to participate in or at least observe exercises, because if policy specialists understand

Figure 2



Source: National Cyber and Information Security Agency of the Czech Republic

A nontechnical tabletop exercise is conducted at the Africa Endeavor Symposium in Ghana in 2019. U.S. AFRICA COMMAND

the aspects of cyberspace through participation in exercises and thus grasp the technical basics, they are better suited for creating policies. However, exercise designers can largely benefit when possessing knowledge of relevant policies on their own. Enable and support their education and self-development in areas other than exercises. Such an approach will pay significant dividends in the future.

- **Selection** — The selection of deficiencies to be identified as blind spots must be commensurate with the nature of national policies and must be prioritized. When the system is not fully developed, prioritization is critical.
- **Whole-of-government approach** — A national cyber security system includes many stakeholders (e.g., critical national infrastructure operators, regulators, internet service providers and law enforcement). In this respect, relevant organizations should be included to address and negotiate over the blind spots. Cyber security at the national level cannot be ensured solely by one dedicated institution. The side effect of this process is to establish trust, which has been essential in the case of the Czech Republic.
- **Consistency** — Ideally, a document addressing the blind spots should be produced regularly since exercises frequently reveal blind spots as well. Presenting such a document annually is frequent enough and sustainable.
- **Offering a solution** — The product should not only draw attention to revealed insufficiencies in the system. It is essential to present solutions based on previous discussions with the relevant entities. Such an approach is significant for subsequent implementation. Unsurprisingly, exercises can be relevant in this process as well. When the blind spot is encountered during an exercise, participants often try to come up with a solution. Sometimes international participants share best practices from their countries. This might represent another precious outcome of the exercise to be included in a blind spots paper.
- **Continuous evaluation** — The evaluation process should work retrospectively and provide honest feedback on the effectiveness of previously applied solutions. The effectiveness of new policies might be a good topic for a new exercise.
- **Keep the circle running** — The ecosystem of identification and sharing the input and output should be never-ending, comprehensive and dynamic because insufficient information sharing or evaluation could generate a new blind spot. ◻

PER CONCORDIAM ILLUSTRATION

Building ALBANIA'S CYBER CADRE

A look at gaps in education, professional training and certification in cyber security

By **Dr. Vilma Tomco**, director general, and **Klorenta Janushi**, information security expert,
National Authority for Electronic Certification and Cyber Security, Council of Ministers, Republic of Albania

Cyber security is a national priority. With the proliferation of communication technologies advancing at such an unprecedented speed, cyber security, interoperability and digital transformation have become the primary topics of the digital world.

Considering the brain drain phenomenon, we are already in a crisis in which we do not produce the number of skilled experts that the industry desperately needs. Investing money may not be the major obstacle it used to be, but organizations still need to map out the resources, assets and the competencies that they have to see what is missing.

The current attitude toward the overall skills shortage is to find short-term patches to the problem. Universities have added cyber security undergraduate or graduate degrees to their curricula. But curriculum designers must recognize the challenges they face as the digital environment evolves at exponential rates. Because of the dynamism of the field, it needs to be well understood that it is fundamentally different from any existing curricula. This understanding is essential to reducing the shortage of cyber security experts, involving more women, and creating more diversity in the cyber domain.

Regulatory framework

The European Union emphasizes the field of cyber security through the development of a common regulatory framework that consists, in part, of the adoption of the Directive on Security of Network and Information Systems (NIS Directive). Albania, as part of its engagement as a candidate for EU membership, has partially adopted the NIS Directive through Law No. 2/2017 on Cyber Security. The law entrusts the National Authority for Electronic Certification and Cyber Security (NAECCS) with oversight and fulfillment, and NAECCS acts as the national Cyber Security Incident Response Team (CSIRT), pursuant to the law. To fulfill these functional tasks, NAECCS has adopted a methodology for the organization and functioning of CSIRTs at the national level. The methodology defines the obligation to establish a CSIRT in each critical and important information infrastructure operator (CIIIO). The list of operators is approved by the Council of Ministers and updated every two years.

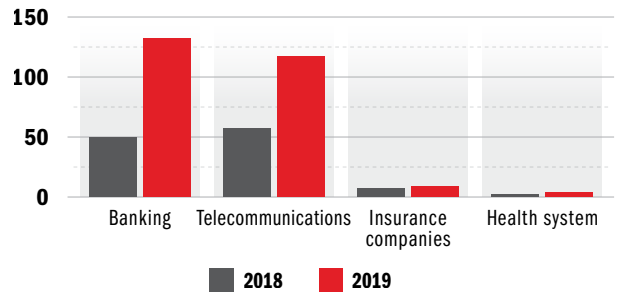
The Law on Cyber Security and its bylaws define the obligation for each CIIIO:

- Create dedicated cyber security positions through the establishment of sectoral CSIRTs.
- Improve system functionalities by implementing additional measures to increase security levels and coordinate with the national CSIRT for real-time handling of cyber incidents.
- Increase the technical and professional capacities of human resources through the organization of specific training in the field of cyber security, cyber drills and so forth.

Enforcement of the law and its bylaws is reflected in Figure 1. After completing the regulatory framework on cyber security, the CIIIOs increased the number of positions dedicated to cyber security. Figure 1 represents some of the most dynamic sectors based on the NIS Directive. NAECCS periodically conducts cyber drills and tabletop exercises to improve the skills of the experts, aiming to create a safer cyber ecosystem in Albania. For the same period, CIIIOs increased their commitment to cyber security projects by investing 1.1 million euros.

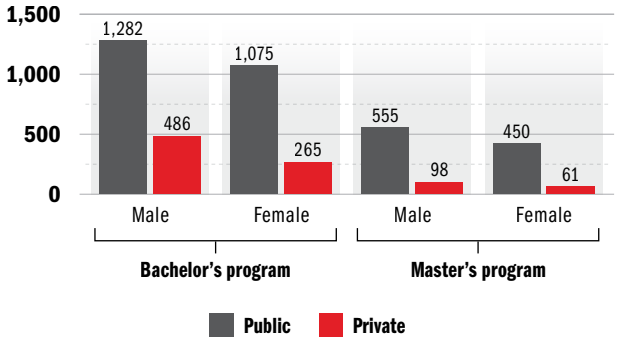
There is a threat common to public institutions that may quietly erode their defenses: cyber security brain drain. Contributing factors are low salaries at public institutions and manual processes for maintaining existing systems — boring manual work for highly skilled experts often results in dissatisfaction and brain drain. The results of the survey found that only 35% of cyber security experts in the sectors analyzed hold a valid international certificate, such as Certified Chief Information Security Officer (CCISO), Certified Information Security Professional or ISO 27001 (International Organization for Standardization).

Figure 1: **Number of cyber security experts in CIIIOs**



Sources: Dr. Vilma Tomco and Klorenta Janushi

Figure 2: **Students studying cyber security in higher education in Albania, 2019**



Sources: Dr. Vilma Tomco and Klorenta Janushi

Water gushes from the dam in Vau i Dejes on the Drin River in northern Albania. A qualified cyber security workforce is essential to protect critical infrastructure, such as this dam. REUTERS

Dea Rrozhani and Jonada Shukarasi, both 16, created GjejZa, an application to fight domestic violence. More women seeking careers in information technology will help offset the human capital shortage. REUTERS

Cyber security students

A survey of institutions of higher education in Albania conducted by NAECCS in 2019 analyzed the student demography, categorized by gender and level of study (bachelor's degrees and master's degrees). Figure 2 shows the difference in the number of males and females and how after graduation, they will increase the level of cyber expertise in the market.

Lectures on cyber security are in 20% of the total curricula in public universities, 15% in private universities and 10% in professional training centers. NAECCS plays a fundamental role in increasing the number of cyber experts in Albania by increasing the number of students trained in the field. Since 2017, NAECCS has organized the Albanian Cyber Academy (ACA), aiming to increase student interest in the field of cyber security. ACA invites local and international experts on cyber security and students of information and communications technology (ICT) to deepen their knowledge and to network within the field.

Every year NAECCS organizes a conference themed "Women in ICT Day" to have successful women from the ICT field share insights and motivate young people to choose a career in cyber security. Women in Albania hold the highest decision-maker positions in ICT, as directors general, CIOs and CISOs.

Conclusions

Organizations have a clear responsibility to improve their information technology security staff training and retention programs, and particularly to attract junior staff. In the future, we will see an expansion of cyber security content across all curriculum, as all students represent potential new entrants into the cyber security workforce. Professional development is critical because the nature of the threat evolves quickly. Professionals can use many options to augment their skills, including certificates, additional university degrees and hands-on courses to develop specific technical skills.

Since university curricula has a long process for approval, professional training centers can help address the needs by organizing short-term courses for information security technicians, analysts and auditors.

As the data in Albania show, women are more focused and loyal to their work, so it is crucial to invest in and attract more women to the cyber security domain. This can be achieved with awareness campaigns and activities, such as competitions, hackathons, conferences and university guidance, among other efforts. ◻

BREAKING the TRIANGLE of DISTRUST

By **Dr. Maximilian Schubert**, secretary-general, Austrian Association of Internet Service Providers

PER CONCORDIAM ILLUSTRATION

Mutual respect and trust are prerequisites for mastering cyber security challenges

For more than 20 years, the majority of online activity was seen as positive, empowering and sparking many beneficial changes for society. Unfortunately, today some people are abusing this technology. Internet service providers (ISPs), law enforcement authorities (LEAs) and civil society have the common goal of making the internet a safer place. However, they address the challenges from different angles: LEAs want to catch criminals, ISPs want to satisfy their customers' needs, and civil society wants to advocate for fundamental rights.

This article builds upon the author's experience as a participant in the Program on Cyber Security Studies (PCSS) at the George C. Marshall European Center for Security Studies in 2017. It aims to illustrate the necessity of a trustful collaboration among stakeholders and tries to outline existing biases.

When attending programs such as the PCSS, it's a great challenge as an industry representative to speak for the whole industry because on most topics there is no common view. Most people might wrongfully assume that the majority of people working in the internet industry share similar cultural views. In reality, cultural and historical influences have a strong effect on their views. For instance, while people originating from established democracies (e.g., the United Kingdom) tend to demonstrate a relatively high level of trust in public institutions and thus might accept a larger degree of public surveillance, people from countries with current and historical reasons to distrust authorities (e.g., Chile) might be significantly more sensitive in respect to privacy and public surveillance.

In the context of the PCSS workshop, the internet industry has been repeatedly criticized for not cooperating sufficiently and has been characterized as contributing to the problem more than the solution. In the discussions it was also evident that many political, social and economic problems were simply projected onto industry. Often, sweeping allegations were made, and it was proclaimed that industry was not willing to "do their bit." It was then seen as almost inevitable that control would be shifted toward government either through increased regulation or a takeover of central functions by public authorities.

A lack of trust was also seen as a factor that is hampering the public sector in its "war for talent." State actors often feel disadvantaged compared to the private sector in respect to their attractiveness as employers, due in part to their rigid employment requirements, salary schemes and confidentiality policies. However, public employers could become highly inventive to obtain desired human resources: While some rely on emotional bargaining, others offer their staff attractive job descriptions, as well as extensive training possibilities and sufficient time in an extremely fast-moving industry to be able to work in detail on technical challenges that arise.

Ideological Differences in a Simulation Game

The tension between privacy, on the one hand, and security, on the other, was a subject that was often raised, but sadly never comprehensively dealt with. The diverging views on this topic were best highlighted within the context of an online simulation game known as CounterNet, a single-player, web-based game focused on how terrorists use the internet and social media for various illicit ends. In this game, players assuming the role of a public authority representative are tasked with tracking and ultimately preventing an attack by a fictional eco-terrorist group. At one point in the game, level advancement was contingent on ordering the observation of the telecommunications of a suspected criminal without a legal basis, thereby knowingly ignoring and intentionally violating fundamental rights. The decision not to give this order resulted in a deduction of points in the game and stopped the player from moving forward to the next level.

During the debriefing, this requirement to break the law triggered a heated debate. While a substantial number of participants refused to act without a legal basis, others showed sympathy for the need to disregard fundamental rights based on the game's scenario of an imminent terrorist attack. As such the simulation did an excellent job, showcasing the different ideologies and attitudes of the various stakeholders and allowing ample time to have an in-depth discussion.

An analyst reviews social media data at the Statewide Information and Analysis Center in Salt Lake City, Utah.
GETTY IMAGES

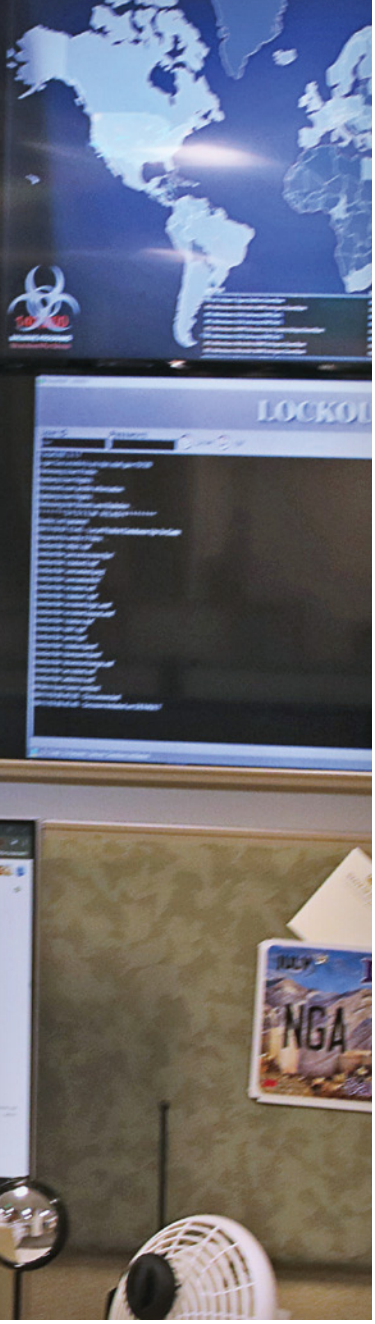
The Triangle of Distrust

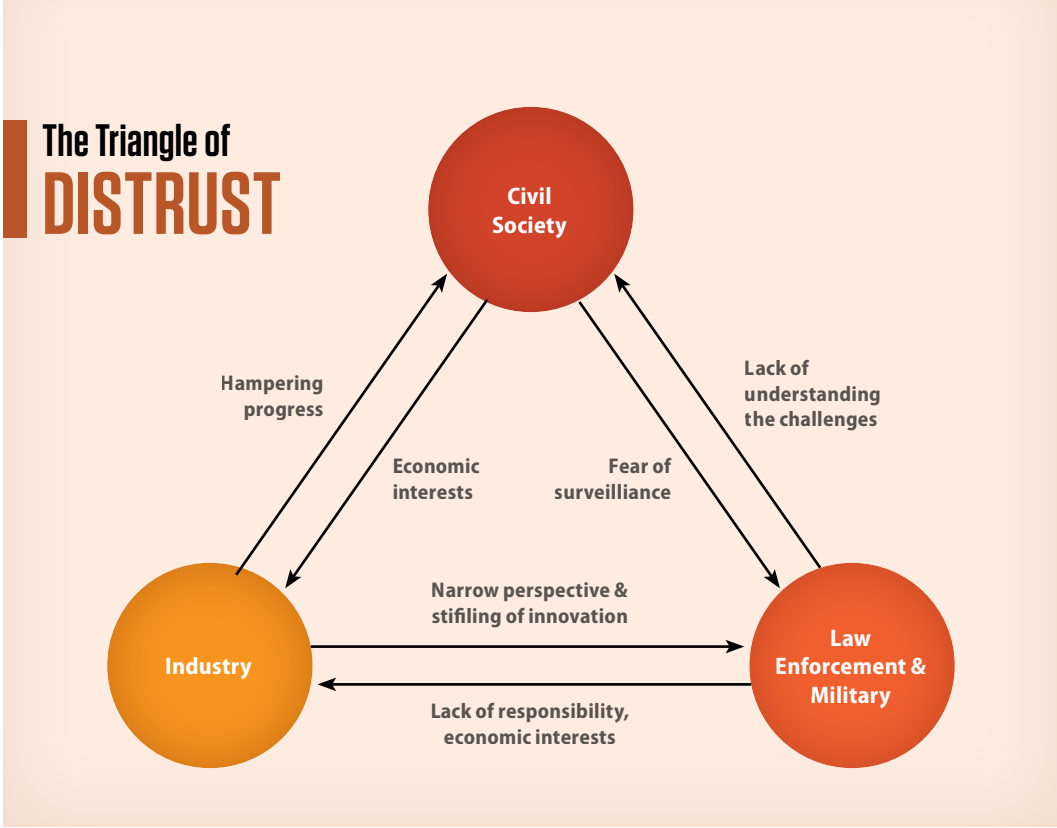
It is not an exaggeration to say that the current relationship between industry, civil society and government agencies around cyber security invokes conflict and misunderstanding. But to achieve the common goal — create a "safe" cyberspace — all actors are dependent on each other. While in the past it has often been sufficient for public authorities to rely on their constitutional authority, in the era of "fake news" and targeted national disinformation campaigns, public actors, such as the military and law enforcement, are under more pressure than ever to justify their actions. These doubts should be met with transparency and a willingness to debate openly.

As long as the three stakeholders of civil society, industry and the public sector (LEAs and the military) keep accusing each other in a blanket and polarizing manner, there will be a lack of mutual respect. Such accusations impede the creation of trust, which forms the basis for the necessary cooperation between all actors that is required to tackle the challenges of the cyber realm. To break down the individual elements of this triangle of distrust, the most common prejudices can be summed up as follows:

Civil society distrusts industry for not being transparent about its motives and the degree of its cooperation with law enforcement. Due to necessary secrecy and a subsequent lack of information available to members of civil society, law enforcement and the military tend to be perceived as institutions exaggerating dangers with the aim of extending their influence and control, thereby threatening civil liberties and, effectively, the democratic system.

Law enforcement and the military accuse civil society of being naive and refusing to accept the reality of challenges in the cyber realm. Industry is criticized for not accepting responsibility for the threats they create, while at the same time using the argument of fundamental rights





not to cooperate with law enforcement.

Industry criticizes civil society for overreacting in respect to privacy and thereby hampering innovation. Law enforcement and the military, at the same time, are sometimes perceived as acting with an overly narrow mindset, ignoring the negative effects their actions could have on business or the further development of the internet and other technologies.

Precisely for these reasons, initiatives such as the PCSS program represent an essential opportunity to identify biases and to subsequently be able to overcome them. To support this process, further expanding the circle of potential program participants should be considered, and representatives of civil society should also be included alongside those of industry. This could help contribute to reducing prejudice among these actors, in addition to establishing greater understanding of the identified prejudices on the part of the military and LEAs.

Trust is a prerequisite for successful cooperation between the internet industry and law enforcement agencies.

While cooperation between industry and LEAs has often been perceived as suboptimal, significant improvement has been achieved by addressing the root causes. Aside from legal and regulatory challenges, surprisingly these are often practical and actionable challenges, as demonstrated by the latest Europol SIRIUS report on cross-border access to electronic evidence, which revealed the most common practical challenges.

The most common challenges for LEAs include not knowing where to turn, not fulfilling the formal requirements (e.g., missing signatures), not providing necessary information (e.g., no valid legal basis) and not knowing how to transfer requests (e.g., LEA insists on sending fax messages instead of emails). To address these issues, a number of European countries, such as the Netherlands, have established specially trained and equipped, national single points of contact for the exchange of information with the internet industry, which has led to a significant rise in successful requests. Another key to their success is the ability to develop a trusted relationship with industry. It can be initiated, for example, by attending the same events as industry members or by inviting them to informal breakfast meetings to discuss practical challenges.

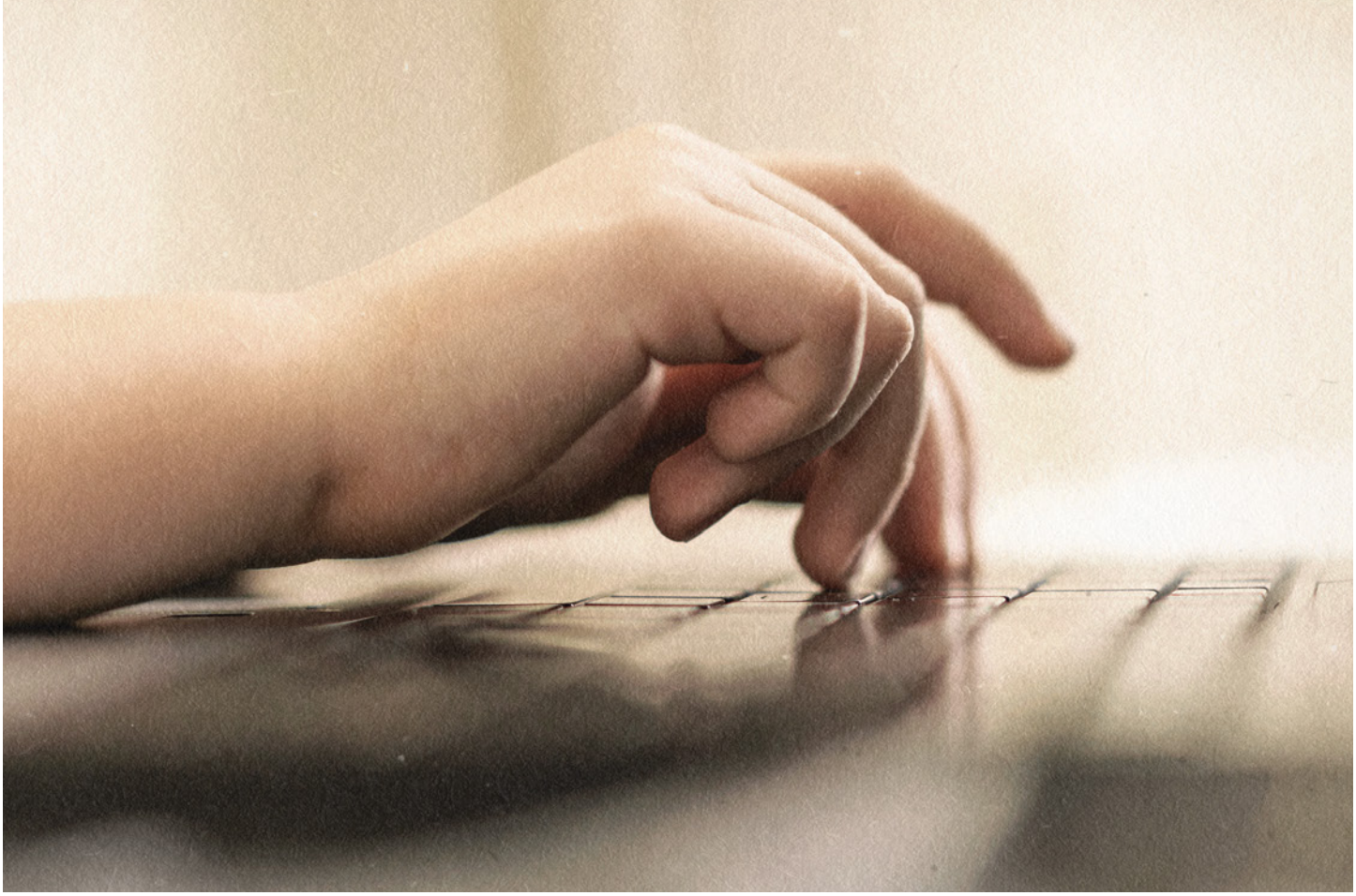
As such, tackling the practical challenges has enabled a new level of cooperation, showing that in almost all cases when ISPs are asked to provide information, a "no" from an ISP does not mean they do not want to help LEAs, but they are not able to help due to technical aspects or legal requirements.

To overcome the differences, while aiming to create a safer cyberspace, serious discussion is needed. Irrespective of how frustrating and resource-draining such a discussion may appear, it may not be bypassed. The PCSS program and the Marshall Center could play a key role in enabling the various stakeholders to build the trust needed to achieve their common goal: a safer internet for every user. Even if opinions about certain topics will differ in the future, a trustful relationship between ISPs, LEAs and civil society facilitates knowledge transfer to obtain this common goal. ◻

SECURING *the* FUTURE

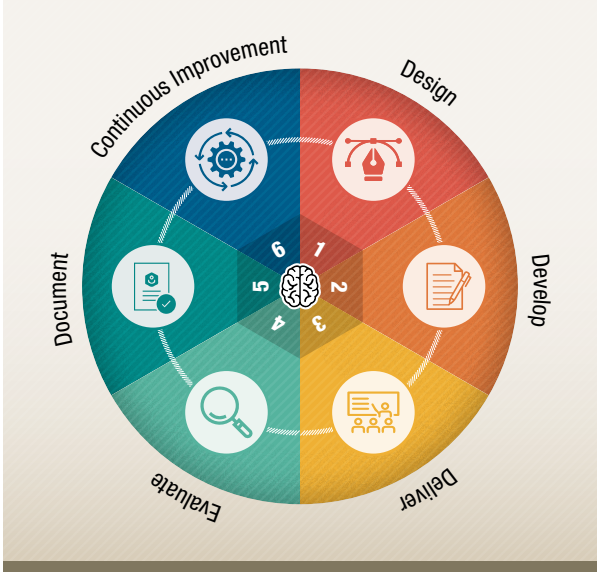
Child Online Protection Action Plan

By **Racky Seye**
Head of the Office of Information Systems Security and Digital Trust,
Senegal Ministry of Digital Economy and Telecommunications



Children and young people are among the most fervent users of mobile technologies. While this can have a positive impact on their education and lives, mobile technologies can also be harmful. Protecting children in cyberspace is as essential as it is in the physical world. Parents, governments and businesses have important roles to play in protecting and supporting connected children and helping them avoid deviant behavior and its detrimental consequences. To address this problem, it was crucial for Senegal to develop a national-level child online protection (COP) workforce and to conduct an action plan.

CHILD ONLINE PROTECTION PLAN



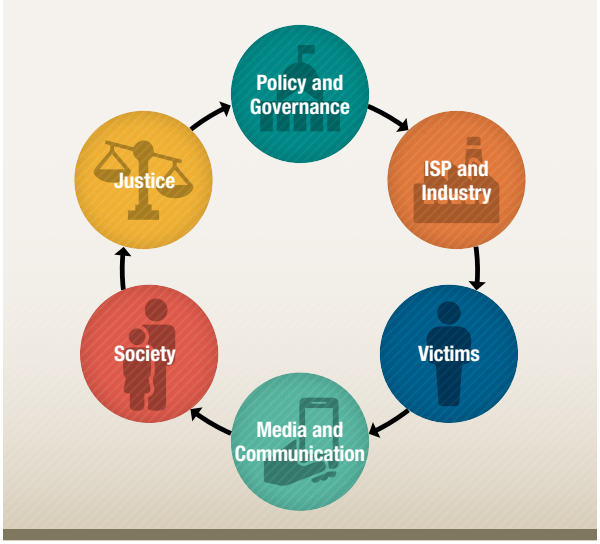
The penetration rate of internet services in Senegal is estimated at 68%. With 10.4 million internet subscribers, 41% of whom are under 15 years old, the government has made COP a priority, counting on the convergence and synergy of initiatives and the strengths of institutions, as well as on families and civic associations.

In this context, the government of Senegal has approved the Senegalese National Cybersecurity Strategy in accordance with the implementation of the Digital Senegal 2025 Strategy. This document aims to establish "a cyberspace of trust, secure and resilience for all" in Senegal by 2022 and also promote a generalized culture of cyber security. It highlights a specific objective: "Raising awareness of all the groups concerned as well as the general public on the security risks in cyberspace."

The National COP Action Plan follows from the implementation of this strategic objective. This plan, which demonstrates the commitment of Senegal to protecting children on the internet, rests on six pillars:

1. Policy and governance
2. Justice
3. Society
4. Media and communication
5. Victims
6. Internet service providers (ISP) and industry

THE SIX PILLARS



Each pillar includes activities — such as awareness-raising and training for children, parents and stakeholders — as well as setting up technical systems to better care for victims to ensure a balance between protecting children in the digital world and empowering them through the use of mobile and information and communications technology (ICT).

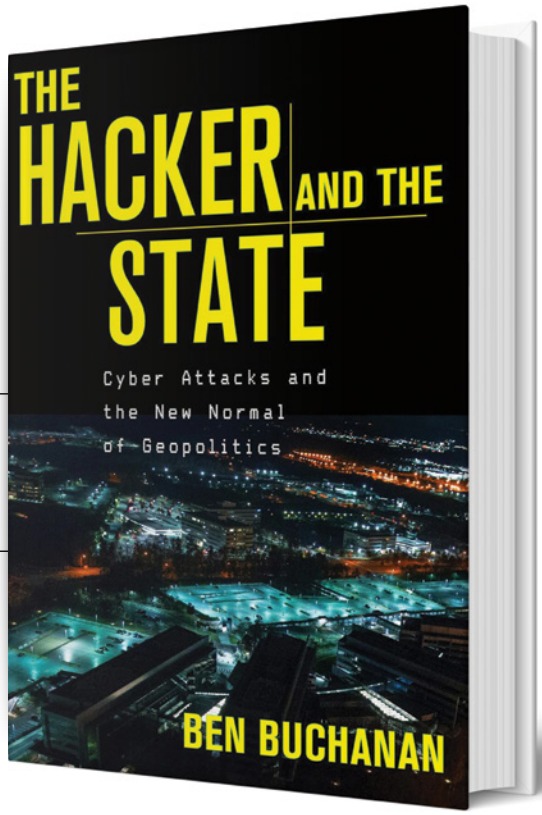
Within the implementation of this plan, in particular Pillar 1 concerning policy and governance, a steering committee of key players in COP from the public and private sectors and civil society was created through ministerial decree. It is chaired by the ICT directorate of the ministry in charge of the digital economy. Its objective is to lead the process of implementing the action plan through regular meetings and seminars.

At the start of each year, the committee uses the action plan to draw up an annual work plan that outlines activities for the year. This committee also serves as an international point of contact on matters relating to protecting children online.

Children and young people are the next generation of cyber-aware leaders, and national programs must address their unique needs now and society's comprehensive risks in the future. Whole-of-government approaches have proven effective. To create the next generation of the cyber workforce, such plans need to be brought to the fore of the cyber policy discussion. ◻

THE NEW NORMAL

AUTHOR: Ben Buchanan
PUBLISHED BY: Harvard University Press
REVIEWED BY: Patrick Swan, *per Concordiam* contributor



Cyber war wasn't supposed to be this way. We expected the digital equivalent of Pearl Harbor, signifying the opening shots in a big global conflict. Like nuclear war, it would present a cyber version of mutually assured destruction. Instead, it has shown to be more effective when employed stealthily and with origin deniability — persistent, annoying, jostling cyber skirmishes. As a form of statecraft, these are more akin to cloak-and-dagger espionage than employment of big, ballistic bombs. There is an irony to this. As digital technology permits ever more precise delivery of conventional munitions, cyber technology remains often a mere blunt, uncontrollable and uncalibrated area-wide instrument of power.

To understand better this uncertain realm of warfare, Ben Buchanan offers us advice in his book, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. He writes: Always keep two approaches to statecraft in mind: signaling and shaping. If one can decipher whether a given cyber operation is intended to signal capability or to shape behavior, one can manage a competent understanding of "what just happened."

One signals an adversary that it has to change a certain behavior or face the consequences, while the other shapes events by hampering an adversary's behavior. Buchanan argues that cyber is an increasingly versatile tool for shaping geopolitics and seizing advantages but is ill-suited for signaling one's positions and intentions. Cyber capabilities often benefit from or require secrecy, he writes. Signaling makes visible one's cyber capabilities.

Buchanan is blunt: The best way to conceptualize cyber operations is not through familiar signaling-centric paradigms, but through the framework of shaping, rooted in concepts such as espionage, sabotage and destabilization. He adds, "The states that reap the most benefits from hacking are the ones that aggressively mold the geopolitical environment to be more to their liking, not the ones that try to hint, coerce, or threaten."

Nations threaten each other with rhetoric all the time. The old saw, "oh yeah, you and what Army" is a truism. You say you can cripple my power grid. Go for it. But unless those words are backed up with action, the threat is interpreted as nothing more than bluster. Even if Country Y acts against Country X, the effects are short-lived. The grid fails and the public undergoes inconvenience or suffering. County X restores the grid with more safeguards. At the same time, Country Y has surrendered its ability to shape County X's conduct.

There are occasions when one may need to inadvertently signal one's cyber capabilities while in the process of shaping. The United States killed the Iranian Revolutionary Guard commander at the Baghdad airport with a precision airstrike. The Americans shaped

the ongoing conflict with Iran with this strike, assessing that removing the Iranian commander provided greater benefits than just signaling their capability to do so. No doubt, the strike led the Iranians to change their movement protocols, but these changes could not bring back an indispensable and charismatic leader.

To help readers comprehend the nuances in signaling and shaping, Buchanan divides his book into sections on espionage, attacks and destabilization. He recalls the message of international relations strategist Thomas Schelling, who focused a theory of warfare on bargaining. Signaling one's "power to hurt" an adversary could coerce the adversary to at least partially bend to one's will to avoid further costs. It sends clear and credible signals. Again, the problem with using this in cyber operations is the signals are rarely clear because by nature they must be shadowy. Hence, rather than signal to Iran that the U.S. had a cyber capability to sabotage its nuclear reactor work if it did not alter its pursuit of a nuclear bomb, it purportedly actually sabotaged it quietly, with the Stuxnet worm. This shaping operation undermined Iranian confidence in its ability to manage a nuclear reactor centrifuge because it did not know for certain whether this was a hostile, cyber-engineered problem or incompetence by its engineers.

In turn, when Iran launched a cyber attack on the Aramco oil company in Saudi Arabia to signal displeasure with Saudi policies, it failed to change Saudi behavior. One reason was that it was done surreptitiously, by third-party hackers, so Iran could deny national involvement. Buchanan states that signals are more meaningful when a state commits to them. Iran did not do so, surrendering the "win" that its hackers had achieved. Another aspect of effective, nuanced geopolitical signaling that Buchanan references is the capacity to inflict carefully measured amounts of violence, with the threat of more to come. After the Aramco strike, the Saudis did not fear a follow-up attack and did not change their behavior to satisfy Iranian objections.

The vignettes Buchanan shares reveal a conundrum for geopolitical cyber operations. Nations use hackers to act on behalf of the state. The state denies involvement so as not to trigger a physical war with an adversary. But the signal can be lost if the attack cannot be traced with certainty to the sponsoring nation. Additionally, if the sponsor nation is not directly overseeing the operation, the signaling may be murky.

Buchanan relates three observed characteristics of hacking: its versatility as a tool of geopolitical shaping, its weakness as a means of geopolitical signaling, and its ambition, which has become increasingly aggressive as modern cyber operations grow in capability. He writes, "Hacking has earned its place in the playbook of statecraft." At the same time, hacking lacks precision because cyber intrusions do not lend themselves to predictable and easily calibrated force; that is, they cannot inflict a carefully chosen amount of harm. This is because cyber attacks are difficult to control with precision. If the attack achieves less than desired, the attackers often can't go back because the capability is either spent or now detected and countered. And this is a key determinant for success: Its operational effects must be both anticipated and able to be ratcheted up over time. Anything less is just launching figurative cyber Scud missiles haphazardly in the hopes of hitting something of value. Effective signaling requires not just communication but also credible commitment. Buchanan writes, "Demonstrated commitment is hard to muster in cyber operations that risk no lives, have unclear paths of escalation, frequently offer no clear last chance to avert conflict, and often become less effective when their preparations are made public."

An old *Looney Tunes* cartoon had one character harmed by another and then deadpanning dryly, "This means war." In cyberspace, by contrast, Buchanan states that policymakers regard cyber operations not as acts of war or even public crises, but rather as part of the everyday digital melee. Nations use it to jostle for geopolitical advantage and are largely uninhibited by norms, treaties or fears of retaliation. This may go a long way in explaining why they are not treated as war — because one would be persistently at war with a number of nations, while at the same time not knowing for certain that one's counterattack was striking at the actual nation behind the cyber operation. Without this certainty, the digital melee is a more inviting prospect.

In one respect, cyber operations fall squarely into what was once called "operations other than war" or "asymmetrical war" or "small war." They can operate as standalone implements for achieving national strategy as part of a broader menu of activities. In another respect, they can work hand in hand with offensive operations by shaping the digital battlefield at the time conventional kinetic operations commence. It won't matter if the capability is revealed because there won't be time for the adversary to counter it before being overwhelmed by physical force. It works in a time-sensitive sense then.

The big takeaway from Buchanan's book is to know what is more effective — shaping over signaling — in the cyber warfare realm. Then one can prepare best one's cyber capabilities and employ them accordingly against known and anticipated threats when they are needed. In practice, this means against a state actor or a state-sponsored hacker activist. We've learned from experience that to confuse *when* to use each is strategic cyber malpractice.

Given that U.S. investments in security, collective defense and regional stability seek to create conditions that minimize conflict and promote opportunities for peace and prosperity, the best outcome one should strive for is one where cyber operations are unnecessary and, like nuclear weapons, rarely if ever used. □

Resident Courses

Democratia per fidem et concordiam
Democracy through trust and friendship

Registrar
George C. Marshall European Center for Security Studies
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
Telephone: +49-8821-750-2327/2229/2568
Fax: +49-8821-750-2650

https://www.marshallcenter.org
registrar@marshallcenter.org

Admission
The George C. Marshall European Center for Security Studies cannot accept direct nominations. Nominations for all programs must reach the center through the appropriate ministry and the U.S. or German embassy in the nominee's country. However, the registrar can help applicants start the process. For help, email requests to: registrar@marshallcenter.org

Check the Marshall Center Website for Updates on Course Schedules

PROGRAM ON APPLIED SECURITY STUDIES (PASS)
The Marshall Center's flagship resident program provides graduate-level education in security policy, defense affairs, international relations and related topics such as international law and counterterrorism. A theme addressed throughout the program is the need for international, interagency and interdisciplinary cooperation.

PROGRAM ON COUNTERING TRANSNATIONAL ORGANIZED CRIME (CTOC)
This resident program focuses on the national security threats posed by illicit trafficking and other criminal activities. The course is designed for government and state officials and practitioners who are engaged in policy development, law enforcement, intelligence and interdiction activities.

PROGRAM ON TERRORISM AND SECURITY STUDIES (PTSS)
This program is designed for government officials and military officers employed in midlevel and upper-level management of counterterrorism organizations and will provide instruction on both the nature and magnitude of today's terrorism threat. The program improves participants' ability to counter terrorism's regional implications by providing a common framework of knowledge and understanding that will enable national security officials to cooperate at an international level.

SENIOR EXECUTIVE SEMINAR (SES)
This intensive seminar focuses on new topics of key global interest that will generate new perspectives, ideas and cooperative discussions and possible solutions. Participants include general officers, senior diplomats, ambassadors, ministers, deputy ministers and parliamentarians. The SES includes formal presentations by senior officials and recognized experts followed by in-depth discussions in seminar groups.

PROGRAM ON CYBER SECURITY STUDIES (PCSS)
The PCSS focuses on ways to address challenges in the cyber environment while adhering to fundamental values of democratic society. This nontechnical program helps participants appreciate the nature of today's threats.

SEMINAR ON REGIONAL SECURITY (SRS)
The seminar aims at systematically analyzing the character of the selected crises, the impact of regional actors, as well as the effects of international assistance measures.

TELL US WHAT YOU THINK

Per Concordiam is launching a series of surveys to explore the experiences of its subscribers and authors.

Use your smartphone to scan this QR Code or go to https://perconcordiam.com/perconcordiam-survey for access options.

Alumni Programs

Christopher Burelli
Director, Alumni Programs
Tel: +49-(0)8821-750-2706
christopher.burelli@marshallcenter.org
Languages: English, Slovak, Italian, German

Alumni Relations Specialists:

Drew Beck
Western Balkans,
Francophone Africa

Languages:
English, French

Tel: +49-(0)8821-750-2291
ryan.beck@marshallcenter.org

Jochen Richter
Western Europe

Languages:
German, English

Tel: +49-(0)8821-750-2814
(jochen.richter@marshallcenter.org

Marc Johnson
Eastern Europe, Caucasus,
Central Asia;
Cyber Alumni Specialist

Languages:
English, Russian, French

Tel: +49-(0)8821-750-2014
marc.johnson@marshallcenter.org

Frank Lewis
Visegrád Four, Baltics, Middle
East, South and East Asia;
Counterterrorism Alumni
Specialist

Languages:
English, German

Tel: +49-(0)8821-750-2112
frank.lewis@marshallcenter.org

Donna Janca
Americas, Anglophone Africa,
Eastern Balkans, Mongolia;
CTOC Alumni Specialist

Languages:
English, German

Tel: +49-(0)8821-750-2689
nadonya.janca@marshallcenter.org

mcalumni@marshallcenter.org

Contribute

Submit articles and feedback to the Marshall Center at **editor@perconcordiam.org**

Subscribe

For more details, or a **FREE** subscription to *per Concordiam* magazine, please contact us at **editor@perconcordiam.org**

Find us

Find *per Concordiam* online at:
Marshall Center: **https://www.marshallcenter.org**
Facebook: **https://www.facebook.com/PerConcordiam**
Twitter: **https://www.twitter.com/per_concordiam**
GlobalNET Portal: **https://members.marshallcenter.org**
Digital version: **https://perconcordiam.com**

The George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany

MARSHALL CENTER