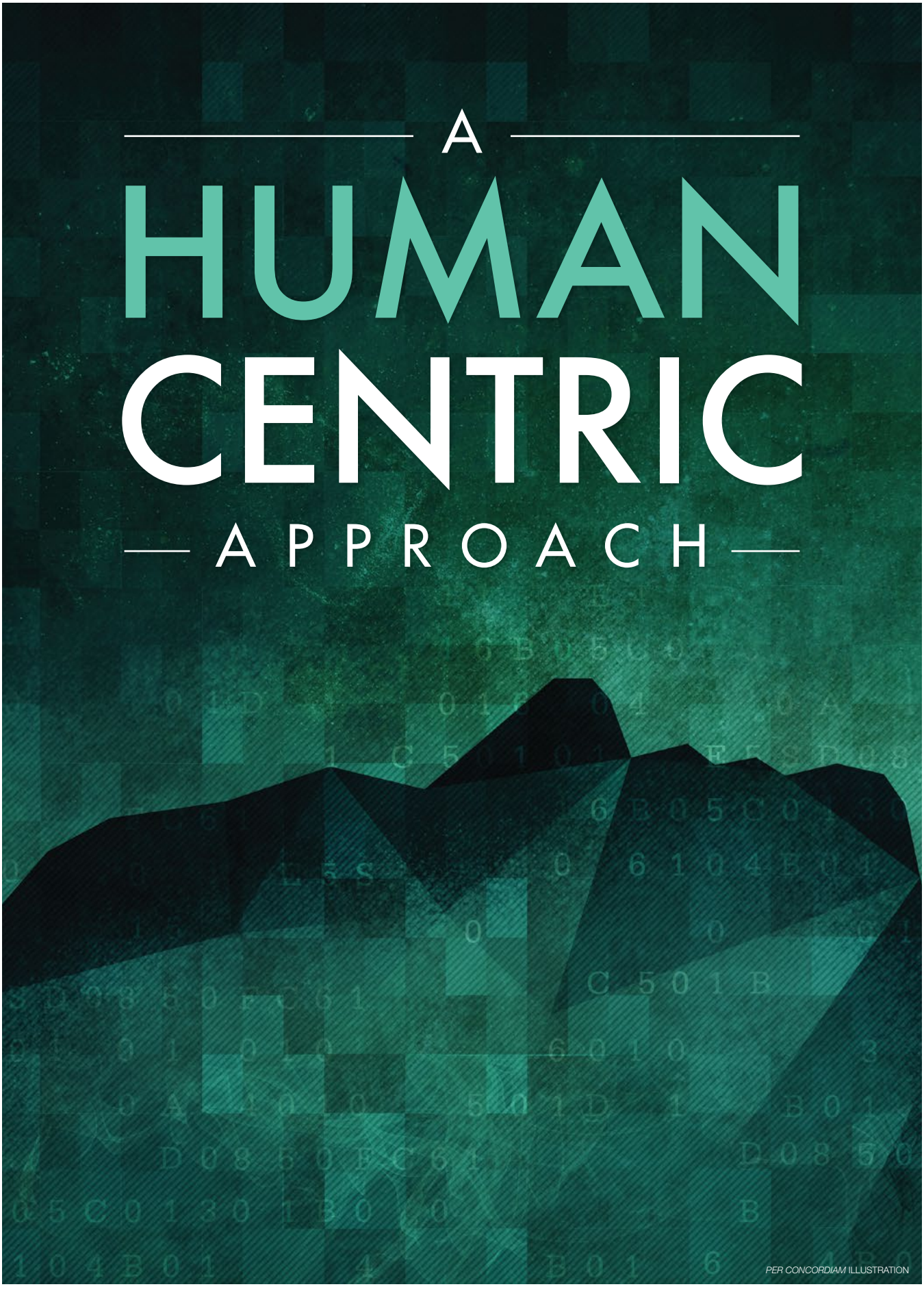
A HUMAN CENTRIC APPROACH



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

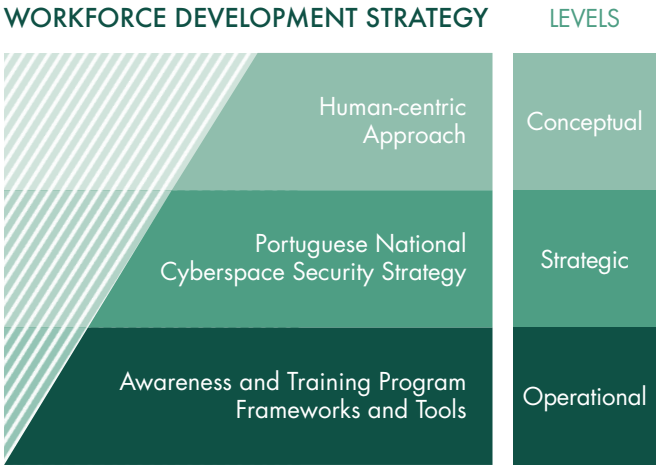
The CNCS' approach starts at the conceptual level, moves to a strategic one, and finishes with operationalization in two domains of action: training and frameworks for autonomous action. These domains must be articulated. That is, the training must reflect the frameworks, and the latter must include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