WORLD ECONOMIC FORUM

Growing Cyber Talent Through Public–Private Partnerships

WHITE PAPER

MAY 2025

Images: Midjourney, Getty Images

Contents

Executive summary

By drawing on the strengths of public and private actors, public–private partnerships can create targeted efforts that advance cybersecurity workforce development.

The rapid evolution of cyberthreats has created a growing demand for skilled cybersecurity professionals. However, many organizations and regions, particularly in the Global South, face significant challenges in attracting, training and retaining talent. Limited resources, brain drain and remote work opportunities leave rural areas and smaller economies more vulnerable in the face of an increasingly complex cybersecurity landscape.

To address these challenges, public–private partnerships (PPPs) are emerging as a promising approach to cybersecurity workforce development. By using the strengths of both public-sector and private-sector actors, PPPs can facilitate targeted initiatives that enhance skills development, expand career opportunities and build sustainable cybersecurity talent pipelines.

The World Economic Forum's Bridging the Cyber Skills Gap initiative has developed this white paper, *Growing Cyber Talent Through Public–Private Partnerships*, to support the design and implementation of PPPs for cyber talent development. This paper explores the key benefits of PPPs for both public and private actors, including financial sustainability, improved access to new markets and the development of critical infrastructure for cybersecurity training and education. At the same time, it highlights important challenges, such as limited awareness of local needs, differing work cultures between sectors and difficulties in aligning long-term goals, all of which can hinder the effectiveness of these partnerships.

To maximize the benefits and overcome challenges, the paper identifies three essential foundations for establishing successful PPPs:

Identifying the right stakeholders: Effective PPPs require selecting appropriate external and internal partners to drive the effort and building trust through transparency and open communication.

Creating tangible outcomes: PPPs should focus on delivering measurable results, such as creating training centres or designing structured training programmes, while remaining adaptable to evolving cybersecurity and workforce needs.

Ensuring effective project management: Strong governance and project execution depend on thorough demand assessments, well-defined roles and responsibilities for all involved stakeholders and performance metrics that drive accountability and long-term success.

Moreover, building on the *Strategic Cybersecurity Talent Framework*, the paper also provides an overview of the different activities that PPPs could undertake to attract talent into cybersecurity, educate and train cybersecurity professionals, recruit the right cybersecurity talent and retain cybersecurity professionals.

By drawing on shared resources and expertise, PPPs can strengthen digital resilience, create employment pathways and play a vital role in building a skilled and diverse cybersecurity workforce.

Introduction

Although nascent in cybersecurity, public–private partnerships can be used to develop talent and create job opportunities.

The cybersecurity landscape is evolving at an unprecedented pace, bringing with it a wave of increasingly complex and sophisticated threats. These threats disrupt the provision of critical services, compromise sensitive data and erode trust across the public and private sectors. In fact, research shows that the cybersecurity skills shortage creates additional cyber risks for 70% of organizations.[1]

Even though the *Future of Jobs 2025* report identifies cybersecurity as one of the fastest-growing skills in the next five years, the global cybersecurity workforce gap remains staggering, with estimates ranging from 2.8 million[2] to 4.8 million[3] unfilled positions. While the talent shortage is a global phenomenon, cybersecurity is unique due to its rapidly evolving threat landscape, the constant need for upskilling, the high stakes of protecting critical systems and data and the growing demand for experienced talent to handle increasingly sophisticated cyberthreats.

The scale of the talent shortage in cybersecurity is further underscored by the World Economic Forum's *Global Cybersecurity Outlook 2025* report, which reveals that only 14% of organizations have the necessary skilled talent to meet cybersecurity objectives. It is important to note that the skills and talent shortage in cybersecurity is not uniform across all roles. Findings by Fortinet show that the most difficult roles to fill are in security operations and cloud security.[4]

Taking a closer look at global cybersecurity talent distribution, data reveals that five countries alone – United States, India, United Kingdom, France and Canada – represent 61% of the world's cybersecurity talent pool. The rest of the world accounts for the remaining 39%.[5] This imbalance highlights how the cybersecurity talent market is largely concentrated in the Global North.

Even though a report by Coursera[6] reveals that cybersecurity is among the top five professional certificates in the Asia-Pacific region, the Middle East and North Africa (MENA) and sub-Saharan Africa, the cybersecurity skills and talent deficit still remains particularly severe, with countries such as Brazil, India, Mexico and South Africa among the most affected. Left unaddressed, skills and talent shortages can create significant challenges. Studies reveal that for 63% of employers worldwide, skills gaps will be the major obstacle to business transformation in the period 2025–2030 and are also likely to exacerbate cyber inequity – the disparity between those with the resources and capabilities to secure their digital environments and those without.[7]

Many organizations in the Global South lack the funding or infrastructure to attract, train or retain top cybersecurity talent. This lack in resources often results in brain drain, ultimately creating a continuous dynamic in which local expertise is lost, hindering efforts to strengthen digital defences.

For example, Deloitte's *Nigeria Cybersecurity Outlook 2025* study[8] shows that the country has faced significant emigration of its cybersecurity workforce – what Nigerians refer to as "japa syndrome"[9] – leaving businesses scrambling to find talent to protect their operations against growing cyberthreats. Some data suggests that Nigeria has only around 8,000 cybersecurity professionals,[10] despite having a population of more than 220 million. Similar challenges are faced by other African countries, including South Africa,[11] but also experienced in other parts of the world such as the Philippines[12] and across Latin America.

In addition to the physical migration of the skilled cybersecurity workforce, many countries are also experiencing a virtual brain drain, where skilled professionals work remotely for international companies without leaving the country. Research suggests that 40% of South African developers work remotely for foreign businesses.[13] As a result, fewer cybersecurity professionals are available to support local companies and public institutions.

While a significant portion of the global cybersecurity talent pool is concentrated in the Global North, another challenge lies in the disparity between metropolitan and rural areas. The Washington DC metro area alone is home to 5% of the world's cybersecurity professionals.[14] Other significant cybersecurity talent hubs are also major technology and government centres, such as New York, London, Paris, Bangalore, the San Francisco Bay Area and Delhi. Similarly, in countries such as France, Germany and Poland, cybersecurity job opportunities are overwhelmingly concentrated in metropolitan areas, where leading enterprises and government institutions are based. In fact, 61% of cybersecurity job postings in these countries are located in major cities,[15] reflecting the strong presence of finance, technology and professional services industries that typically cluster in urban centres. This urban concentration creates significant challenges for smaller cities and rural regions, which often struggle to attract and retain cybersecurity professionals, leaving critical industries and government services in these areas more vulnerable to cyberthreats.

Against this backdrop, governments, companies and international organizations are putting much effort into building public–private partnerships (PPPs) to address cybersecurity challenges, including talent shortages. PPPs have already proven successful in other areas, such as healthcare and infrastructure development. In the context of digital skills development, notable examples of PPPs include a private telecommunications provider in Kenya[16] partnering with UNESCO and the Eneza Foundation to launch a digital mentorship programme, providing STEM career guidance through television, radio and text messages. Similarly, in Saudi Arabia, an edtech company in collaboration with the Ministry of Education has supported around a thousand teachers in their professional development through free online professional development courses, with an option to pay for certifications.[17]

While still nascent in the field of cybersecurity, by using the strengths of both sectors, PPPs can enable the creation of initiatives to cultivate home-grown cybersecurity talent and promote employment opportunities.

1 Defining public–private partnerships

Each public–private partnership is inherently unique, shaped by the specific context, objectives and challenges it seeks to address.

The World Economic Forum Growing Cyber Talent Through Public–Private Partnerships working group defined a PPP as a "collaborative and outcome-based effort whereby public and private organizations share resources, responsibilities and risks in order to advance a common goal, such as delivering a service or a project". Put differently, it is a mutual exchange where both parties contribute valuable resources and gain essential benefits in return.

Whereas traditional PPPs are often characterized by a revenue regime that ensures a source of revenue for the private actor to recover its investment, in the context of cybersecurity talent development, PPPs are often driven by a common goal of collaborative endeavour to achieve greater security rather than by direct financial profit. These collaborations manifest as efforts to design, fund and deliver joint programmes, where each stakeholder may provide financial support or in-kind contributions such as facilities, technology, expertise and personnel. Additionally, partnerships may provide branding, operational support and outreach capabilities, such as using their combined convening power to bring stakeholders together.

In PPPs, public and private actors include:

- Government agencies (e.g. government, ministries, national cybersecurity agencies, law enforcement agencies, etc.)
- International organizations and development institutions
- Businesses or for-profit organizations such as private companies (e.g. cybersecurity firms)
- Not-for-profit civil society organizations
- Public and private universities and training centres
- Industry associations

It is important to note that private companies vary in size and capacity, ranging from large multinational corporations to small and medium-sized enterprises (SMEs). While large companies may have extensive resources, specialized expertise and the ability to invest in long-term initiatives, SMEs often bring agility, innovation and niche expertise but may face financial or operational constraints. These differences can affect a PPP's structure, as smaller firms may require additional support or incentives to participate effectively, while larger corporations might take on more significant roles in, for instance, funding or training.

PPPs can be categorized as either strategic or opportunistic. Strategic partnerships focus on achieving broader socioeconomic outcomes and are carefully integrated into long-term strategies. Opportunistic partnerships, on the other hand, are often reactive and intended to address an immediate need. As such, they may lack alignment with broader strategies.

2 Why choose a PPP?

Public–private partnerships help create win-win scenarios, combining resources and expertise for maximum impact.

As indicated by the definition, public–private partnerships bring together the strengths of both sectors to tackle challenges neither can solve alone. In an interconnected world, cybersecurity is a team sport. Securing digital assets requires collaboration across organizations, industries and geographies, as no single entity can fully protect itself against evolving cyberthreats on its own. Failure to advance cybersecurity, including the development of a skilled cybersecurity workforce, can significantly harm economic opportunities, especially in the Global South. Without adequate protection and talent, these regions face heightened vulnerabilities that can undermine digital growth, deter investment and widen global inequalities.

PPPs help create win-win scenarios, combining resources and expertise for maximum impact.

For public actors, the benefits of PPPs include:

Increased financial sustainability and shared investment burden: Developing cybersecurity talent is resource-intensive, requiring significant investments in training, infrastructure and specialized educators. Estimates suggest that the cost of cybersecurity bootcamps per individual ranges between $10,000 and $18,000.[18] PPPs help mitigate financial strain by securing private-sector investment, enabling long-term funding and reducing reliance on public budgets.

Training quality and relevance: Public actors can benefit from the support of private actors who bring their expertise and the latest knowledge in cybersecurity to the table. Private partners play an important role in helping align education programmes in schools and universities with industry needs, ensuring that students who later progress to becoming cybersecurity professionals are equipped with the skills required to be job-ready.

Creation of new and long-term infrastructure and training facilities: Public actors can use private-sector investments to develop training infrastructure, such as cyber ranges (that is, virtual environments for cybersecurity training) simulation labs and training centres. These facilities provide hands-on experience for learners, improving workforce readiness while strengthening national cyber resilience. By partnering with private entities, public actors can reduce upfront costs, accelerate development timelines and ensure suitable training environments.

For private actors, the benefits include:

Access to new markets: The *Allianz Risk Barometer 2025*[19] finds that cybersecurity is a top concern in Brazil, Nigeria and South Africa, all of which are also facing significant cyber talent shortages.[20] Often, for private actors, PPPs provide access to untapped markets that may otherwise be difficult to reach and, as such, can help open doors to new growth opportunities.

Wider reach: The cybersecurity workforce lacks a representation of diverse groups. According to a 2024 survey by ISC2,[21] 11% of cybersecurity teams have no women, with the lowest representation in energy, military and manufacturing. Additionally, underrepresented groups – including minorities and neurodiverse individuals – continue to face barriers to entry. PPPs enable private-sector organizations to reach larger and more diverse populations by using public-sector networks and education systems to train, recruit and integrate more diverse professionals into the workforce.

Scaling efforts: PPPs provide a valuable opportunity to scale cyber talent development initiatives. Public actors, through strategic policy support, can create the necessary conditions to implement and scale such efforts across industries or economies.

3 Common challenges for PPPs

Challenges, including resistance to external assistance or a lack of mutual trust, can hinder collaboration between public and private actors.

Despite the many benefits of public–private partnerships, they can be challenging to establish or sustain. Even with a 75% surge in global cyberattacks in the third quarter of 2024 compared to the same period in 2023, many decision-makers still underestimate the scale of cyberthreats and the urgent need for skilled cybersecurity professionals, leading to cybersecurity being deprioritized in policy. Moreover, challenges such as resistance to external assistance or a lack of mutual trust further hinder collaboration between public and private actors. In the context of cybersecurity talent development, the following barriers to public–private partnership are worth highlighting:

Differences in working speeds: The private and public sectors often operate at different speeds, which can present challenges to effective collaboration on cybersecurity talent development. While private entities typically move quickly, the public sector, with its approval cycles, regulatory requirements and governance structures, tends to progress more slowly. Finding ways to align the pace of both sectors is essential for ensuring effective collaboration.

Misperception of intent and resistance to external assistance: There is often scepticism about the motives of private-sector involvement in public programmes and initiatives. Questions may arise about whether private-sector actors are genuinely committed to creating positive change or are primarily motivated by marketing, corporate social-responsibility goals or profit. This mistrust can erode confidence in PPPs, making it harder to achieve effective collaborations.

Limited access to public-sector stakeholders: Engaging with the public sector on cybersecurity talent development can be challenging due to restricted access, bureaucratic structures or unclear points of contact. Private-sector organizations may struggle to identify the right stakeholders to initiate collaboration. Additionally, some public institutions may be hesitant to engage with private entities due to concerns over differing priorities or objectives.

Lack of awareness of local context and needs: Global cybersecurity initiatives often fail to account for the unique contexts and challenges faced by local communities. A one-size-fits-all approach that overlooks local economic, cultural and technological realities risks being ineffective or even counterproductive. For example, training programmes designed for developed countries may not be suitable in regions with limited internet access, outdated infrastructure or low levels of digital literacy, further hindering talent development in these areas.

4

Foundations of success for PPPs

The success of a public–private partnership depends on the agility of the partners involved.

Public–private partnerships offer an effective approach to combining the strengths of both sectors to advance cybersecurity talent development. They are particularly valuable when private-sector expertise and resources complement public policy objectives. They work best for initiatives with a clear commitment from both parties, where the goals, benefits and responsibilities are well aligned.

However, every partnership is unique, and tailoring each one ensures the objectives of all involved partners are clearly understood and that resources are allocated effectively. While organizations may engage in multiple partnerships simultaneously, managing them in a meaningful and focused way can often be challenging.

It is important to note that the success of a PPP depends on the agility of the partners involved. Agility allows both public- and private-sector entities to navigate the complexities and uncertainties that may arise during the course of the partnership. At the same time, partners should not go beyond the limits of their ability. Overextending can lead to inefficiencies and unmet expectations that can hinder the success of a partnership. Therefore, agility should be balanced with a realistic understanding of each partner's strengths and limitations.

A PPP should be built on solid foundations that can help deliver impactful solutions and achieve long-term success. Although each partnership has unique needs and circumstances, three foundations have been identified as essential for establishing successful PPPs:

Assemble the right stakeholders: Successful PPPs depend on assembling the right mix of stakeholders. For this to happen, private-sector actors must have a clear understanding of the roles and responsibilities of public entities involved in cybersecurity, including their efforts in cybersecurity skills and talent development. Likewise, public-sector entities should identify private-sector partners who can provide the resources, expertise and training to support cybersecurity workforce development. Assembling the right stakeholders also means that both the public and private sectors must identify the essential internal stakeholders within their organizations – such as executive leadership, finance, legal, HR and others – who will lead the initiative and ensure organizational buy-in and support. This is crucial for maximizing the effectiveness and success of a PPP. Moreover, each partner involved in the PPP must clearly understand the benefits they will gain from the collaboration, whether through policy achievements, financial returns or contributions to societal goals.

Creating a sustainable mechanism: To achieve lasting impact, partnerships must prioritize the development of concrete, sustainable mechanisms such as the establishment of cybersecurity training hubs or centres of excellence to provide continuous upskilling opportunities that extend beyond short-term training efforts. Similarly, using PPPs to integrate cybersecurity training into primary and secondary education and university curricula ensures that cybersecurity skills become a standard part of education, creating a steady pipeline of skilled professionals and reducing reliance on short-term bootcamps. Moreover, provision of mentorships and apprenticeships through PPPs, and their integration into long-term workforce development strategies, ensures that these programmes remain a consistent and effective source of skilled talent.

Effective project management: Effective project management is crucial for the success of a PPP. A vital step in ensuring that a partnership is targeted and impactful is conducting demand studies. These studies can help identify, for instance, cybersecurity skill shortages, education gaps and emerging industry needs, allowing PPPs to tailor their efforts to address actual challenges. By grounding PPPs in real-world data, stakeholders can align their focus strategically, ensuring that efforts are directed at the most critical issues. In addition to demand studies, for a PPP to be truly effective, all stakeholders must agree to a shared objective while tasks and responsibilities must be clearly defined and aligned with each partner's unique strengths. A well-structured division of labour prevents overlap or duplication and ensures that each partner is contributing in a way that fully realizes their expertise. Clear roles achieve efficiency and effectiveness in the partnership. Finally, the success of any PPP is ultimately measured by its ability to deliver tangible, measurable results. Establishing clear performance metrics is essential for tracking progress and identifying areas for continuous improvement. These metrics provide a foundation for assessing the partnership's effectiveness and making adjustments as needed to meet long-term objectives.

5

Examples of how PPPs work in practice

Activities may span from co-designing school curricula on cybersecurity to technology transfer.

Public–private partnerships in the context of cybersecurity can be structured around a wide range of activities, depending on the goals and needs of the stakeholders involved. According to a study by ENISA,[22] these activities may involve cybersecurity incident handling and crisis management, information exchange, exercises and the development of good practices.

In the context of cybersecurity talent development, building on the *Strategic Cybersecurity Talent Framework*, below are a number of illustrations of how PPPs can be used to attract talent into cybersecurity, educate and train cybersecurity professionals, recruit the right cybersecurity talent and retain cybersecurity professionals.

FIGURE 1 **The Cybersecurity Talent Framework**

Source: World Economic Forum. (2024, April). *Strategic Cybersecurity Talent Framework*. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

5.1 Attracting talent into cybersecurity

A concrete example of a PPP attracting talent into cybersecurity can be seen in collaborative awareness campaigns aimed at promoting cybersecurity careers and encouraging talent development across communities.

CASE STUDY 1

Telefónica and the Agency for the Technological Modernization of Galicia

In 2011, the Agency for the Technological Modernization of Galicia (AMTEGA) was created to drive digitalization in the Spanish region. In 2020, AMTEGA partnered with Telefónica to raise awareness of cybersecurity and data protection among the citizens of Galicia and assist local government bodies in preventing cyberthreats and ensuring regulatory compliance.

The main achievements of the PPP include:

- Developing and launching Galicia's cybersecurity web portal, offering educational and informative content.
- Collaborating with regional TV to produce short cybersecurity videos, one of which introduced a cybercriminal character whose name became Galicia's 2023 Word of the Year.
- Organizing more than 600 live lectures, reaching 15,000-plus people, including specialized sessions for seniors.
- Building a strong social media presence, attracting 250,000-plus followers and accumulating 4.3 million-plus views.
- Hosting an annual Girls' Talent in Cybersecurity event to encourage young women to explore careers in cybersecurity.
- Providing resources and advanced tools such as security information and event management (SIEM), automated penetration testing, vulnerability analysis, digital surveillance and consultancy services for data protection and information security.

The partnership optimizes public-fund investments by delivering tangible projects. Services are implemented swiftly, using specialized personnel and the support of a technology company to develop solutions tailored to the needs of the Galician population and local institutions.

CASE STUDY 2

Cyber Education Center

The Cyber Education Center (CEC) is bridging Israel's cyber skills gap while driving social mobility through its flagship programme, Magshimim. As the country's premier cybersecurity education initiative for high-school students, Magshimim is designed specifically for gifted underprivileged youth from Israel's geo-social periphery. It provides cutting-edge training, immersive hands-on experiences and specialized tracks in fields such as artificial intelligence (AI).

Beyond technical expertise, the programme encourages critical soft skills – teamwork, problem-solving and resilience – preparing students for careers in cybersecurity and high-tech industries. With a holistic support system, Magshimim nurtures students beyond tech, ensuring both personal and professional growth. Many alumni return as mentors, building self-sustaining tech environments in their communities.

The programme is further amplified through strategic partnerships with leading private-sector organizations, such as Google, Check Point and Amdocs, which provide resources such as mentorship, industry exposure and office space for hackathons.

With more than 5,500 students enrolled annually and 4,000 graduates – 85% of whom have already successfully integrated into the high-tech industry – Magshimim is not only fuelling Israel's global leadership in cybersecurity but also developing the workers of Israel's periphery, ensuring that talent, not background, defines success.

Ideas to inspire

In addition to large-scale awareness campaigns to promote cybersecurity as an impactful career choice, other possible activities undertaken as part of a PPP may include:

- Co-organizing and sponsoring cybersecurity challenges, hackathons and Capture the Flag (CTF) competitions at local, national or international levels. To illustrate, in 2022, the government of Rwanda partnered with a private telecommunications company to advance the information and communication technology (ICT) skills, including cybersecurity, of more than 10,000 university students across sub-Saharan Africa.[23] Such partnerships allow the public sector to contribute venues or support for hosting large-scale competitions. The private sector can provide the equipment and tools needed to host the events, as well as its expertise to design and run the challenges.
- Hosting employment fairs such as the Road2Cyber Job Fair,[24] operated by the European Cyber Security Organisation (ECSO), and Women4Cyber, with the sponsorship of a private company, where jobseekers can connect with companies in the industry, while recruiters can efficiently identify potential candidates. Public actors can offer spaces for hosting the event or can help promote it – through, for instance, schools and colleges – to attract students and jobseekers. The private sector, for its part, can support with the delivery of live demonstrations, panel talks, etc.

5.2 Educating and training cybersecurity professionals

Some of the most prominent examples of PPPs in cyber talent development are collaborations between public and private organizations to educate and train the next generation of cybersecurity professionals. As illustrated in the case studies below, activities may range from co-designing curricula, developing teaching resources and setting up physical and virtual labs for hands-on training. The public sector can provide infrastructure, funding and regulatory support, while the private sector can contribute technology, realistic threat simulations and practical exercises to equip learners with essential cybersecurity skills.

CASE STUDY 3

Smart Africa Innovation Centre

In April 2023, Smart Africa, in collaboration with the Ministry of Communication and Digital Economy of Côte d'Ivoire, inaugurated an Innovation Centre in Abidjan. The centre is supported by École Supérieure Africaine des Technologies de l'Information et de la Communication and Hitachi Systems Security.

The objective of the Innovation Centre is to build capacity in the cybersecurity sector across Africa. More specifically, it aims to provide training on cybersecurity skills to teachers.

Each stakeholder involved in the partnership has a clearly defined role and responsibility. To illustrate, the private sector is responsible for resource mobilization and the provision of equipment to the centre, the ministry ensures oversight of the initiative and Smart Africa provides training content.

CASE STUDY 4

Trellix Emerging Students Cybersecurity Academy (TESCA)

The Trellix Emerging Students Cybersecurity Academy (TESCA) is a PPP focused on cultivating the next generation of cybersecurity professionals. Through its programme, Trellix collaborates with universities, with the primary objective of augmenting and expanding learning opportunities for students pursuing STEM education and, specifically, cyber-focused degrees or certificates.

Trellix contributes its expertise through hands-on workshops and training sessions, covering real-world scenarios such as incident response, blue/red-team exercises and malware analysis. University partners facilitate student participation and provide academic context. The programme has engaged more than 200 students to date, equipping them with practical cybersecurity skills and knowledge. TESCA aims to broaden its outreach to additional universities throughout 2025, further amplifying its impact on cybersecurity talent development. As Trellix connects with students in TESCA it builds relationships and a pipeline for its early-career talent programmes, including internship and apprenticeship programmes that offer hands-on, real-world experience for students while they work on their programme degrees.

CASE STUDY 5

WB3C-UTT Partnership on Digital Forensics

The Western Balkans Cyber Capacity Centre (WB3C) and the University of Technology of Troyes (UTT) have partnered on a digital forensics programme to tackle the cyber skills gap. The 11-week programme, adapted from UTT's N-Tech course, provides hands-on training to police investigators on cybercrime. WB3C, funded by France, Slovenia and Montenegro, offers trainers and facilities and covers travel and accommodation costs, while UTT supplies the curriculum and instructors. Each participant receives a laptop with installed specialized forensic software and, upon passing a final exam, a recognized qualification.

This programme directly addresses the immediate shortage of skilled cybercrime investigators and digital forensics experts by upskilling professionals already in the field, reducing case backlogs and enhancing law enforcement capacity. As the progress of Western Balkans states towards EU accession primarily relies on judicial reforms, the need to enhance the institutional and operational capacities of law enforcement and achieve full interoperability is a priority.

To ensure long-term impact, WB3C and UTT are working to embed the digital forensics curriculum into local university programmes. University faculty members have been invited to participate in the current course to familiarize themselves with the content and methodology, enabling them to deliver the programme to future generations of students. This approach, resembling the train-the-trainer model, aims to institutionalize digital forensics education and create a lasting pipeline of qualified cyber professionals. The programme also engages accreditation bodies, police academies and other essential stakeholders to develop a standardized and sustainable educational framework. The WB3C-UTT partnership exemplifies how public and academic sectors can collaborate to address both immediate skills shortages and long-term capacity building.

Ideas to inspire

To educate and train cybersecurity professionals, PPPs could also assist with:

- Provision of scholarships and financial assistance to individuals facing financial barriers to pursuing advanced education or certifications in cybersecurity. For example, back in 2013, the United Kingdom government partnered with an IT services and consulting company to provide cyber policy scholarships.[25] Whereas the private-sector entities can offer grants or subsidized certification programmes to make training and education more accessible, public actors can help raise awareness about available scholarship opportunities or track the outcomes of scholarship programmes, ensuring that they are successfully supporting students in both their education and career goals.

5.3 Recruiting the right cybersecurity talent

Recruitment of cybersecurity professionals can be hindered by challenges such as insufficient pools of new graduates. In South Africa, the lack of education and training at a basic level as well as the migration of skilled labour are said to contribute to the skills gap.[26] Organizations in Latin America also struggle to recruit talent, with 80% of organizations in the region struggling to find people with technology-focused certifications, according to Fortinet.[27]

That said, as shown by the examples below, PPPs can be used to improve the recruitment of cyber talent, including that of underrepresented groups such as women, youth and economically disadvantaged communities, helping to create a more inclusive and diverse cybersecurity workforce.

CASE STUDY 6

Her CyberTracks

Her CyberTracks is a global initiative designed to bridge the gender gap in cybersecurity by equipping women with essential skills and opportunities to succeed in the field. Her CyberTracks offers a comprehensive five-month curriculum that includes technical and soft-skills training, mentorship and inspirational networking events.

In 2023 and 2024, Her CyberTracks trained 300 participants, achieving a 93% satisfaction rate and creating a vibrant network of cybersecurity professionals across Europe and Africa. By enhancing participants' expertise and confidence, the initiative strengthens global cyber resilience and creates an inclusive cybersecurity workforce.

The programme is based on strong partnerships: while funded primarily by the German Federal Foreign Office and supported by Microsoft, the initiative is co-implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), the International Telecommunication Union (ITU) and the United Nations Office on Drugs and Crime (UNODC). Local collaboration is also integral, with the Latin America and Caribbean Cyber Competence Centre (LAC4) supporting regional implementation, and public- and private-sector partners contributing in kind to the curriculum.

This partnership model uses the strengths of each entity: international organizations provide strategic guidance and lead the implementation; private-sector partners offer industry expertise; and financial contributors ensure programme scalability.

CASE STUDY 7

IDB: Promoting Cybersecurity and Youth Employment in Panama

The Inter-American Development Bank (IDB) is supporting, through financing, the promotion of cybersecurity and youth employment in Panama. The objective of this PPP is to develop skills and create jobs related to cybersecurity, focusing on improving women's participation in the sector and expanding access to affordable cybersecurity services for SMEs.

The entities involved in this alliance include NUMU Corporation, Deloitte Cyber Academy, Technical Superior Specialized Institute (ITSE), MNEMO Cybersecurity and various other organizations. NUMU Corporation is responsible for project management, skills development, bridges to employment and funds administration, while MNEMO Cybersecurity provides technical services and market experience. Deloitte Cyber Academy offers an online learning platform, while ITSE and other organizations assist in the outreach to young participants and host important activities related to the project.

The impact of this alliance includes the establishment of a cybersecurity centre of excellence, the training and certification of 406 youngsters, 40% of them women, work experience for 200 of these individuals and the provision of cybersecurity services to 300 SMEs, enhancing their resilience to cyberattacks. NUMU is expanding this concept to El Salvador and other countries to open the highway of digital transformation opportunities for more people in the region. The goal is to make an impact through cybersecurity labs and AI skills development roadmaps, targeting the more vulnerable population in that country.

CASE STUDY 8

Cisco Academy and Edge Centres in South Africa

PPPs in cybersecurity offer a unique opportunity to enhance workforce development and drive economic growth. Cisco's Networking Academy exemplifies this by equipping individuals with critical digital skills. Active since 1998 on the African continent, it trained more than 260,000 students in cybersecurity in 2024 alone in collaboration with schools, technical colleges, polytechnics and universities. And it doesn't stop there. In addition, in collaboration with the South African government, the Edge Centre initiative supports small, medium and micro enterprises (SMMEs), which are crucial for innovation and job creation.

This programme in South Africa is a strategic initiative under Cisco's Country Digital Acceleration (CDA) programme, designed to drive digital transformation, innovation and skills development. This initiative addresses unemployment and skill shortages, aligning with national Memorandum of Understanding and the Broad-Based Black Economic Empowerment laws to promote economic inclusion and transformation. Edge Centres provide SMMEs with advanced Cisco technology and training, connecting them with global Cisco experts. This partnership transforms SMMEs into specialized technology partners and links Networking Academy graduates with employment opportunities, meeting business talent needs. This partnership highlights the transformative potential of PPP in cybersecurity, promoting innovation, economic growth and developing a future-ready workforce.

Ideas to inspire

To promote the recruitment of cyber talent, PPPs could also help:

- Launch apprenticeships and bootcamps: cybersecurity apprenticeships, bootcamps, hackathons and other training or competition programmes introduce aspiring professionals to the field and help them build foundational skills quickly. To ensure a steady supply of cybersecurity experts in critical national infrastructure (CNI), the United Kingdom government, in collaboration with a number of private-sector entities, ran the Cybersecurity CNI apprenticeships programme in 2017.[28] Similarly, in 2023, the Communications Authority of Kenya partnered with the private sector to equip students with cyber skills through bootcamps and hackathons.[29] The public sector can provide financial incentives such as grants to encourage companies to establish such programmes, while the private sector can play a leading role in designing the scope of apprenticeships and cybersecurity challenges.
- Create programmes that facilitate the mobility of cybersecurity professionals across borders: the public sector could play a role in developing and implementing such programmes. This could include specialized visas for cybersecurity professionals, such as the Global Talent visa programme in the United Kingdom,[30] or simplification of other bureaucratic processes related to work permits and residency requirements for cybersecurity professionals. The private sector could offer incentives including relocation packages, remote work options and visa sponsorship.

5.4 Retaining cybersecurity professionals

While cybersecurity talent retention – both within organizations and across national economies – is a global challenge, research suggests that it is particularly critical in the Global South due to the brain drain trend.[31] In Latin America, India and Africa, for example, 69%, 66% and 65% of organizations respectively struggle to retain talent. In North America this figure drops to 45%.

PPPs can play a role in advancing professional development and create a positive work environment to keep cybersecurity professionals engaged and committed, helping to avoid talent loss.

CASE STUDY 9

Fortinet and the Ministry of Higher Education, Scientific Research and Professional Training of Morocco

Morocco is working towards a new era of progress and modernization aimed at enhancing the quality and efficiency of the Higher Education, Scientific Research and Innovation (ESRI) environment. The nation is relying on younger generations to serve as a catalyst for advancing its developmental progress.

The National Plan for Accelerating the Transformation of the ESRI Ecosystem (PACTE ESRI 2030) was launched by the Ministry of Higher Education, Scientific Research and Professional Training. The plan involves three main strategies: digital transformation, regulatory framework adaptation and national and international partnership opportunities.

Fortinet joined the initiative in 2023 and has been working with the ministry under Code 212: An Innovative Network for Training the Digital Talent of Tomorrow. Code 212 aims to develop young people's technological skills, encourage innovation and facilitate the country's digital transformation. It also seeks to strengthen the tech environment and enhance youth employability.

It offers training in four vital areas: coding, data, cybersecurity and systems and IoT (internet of things).

Fortinet provides cybersecurity training and certification, at no cost to this initiative, through its Academic Partner Program. Through this partnership, Fortinet is actively supporting Code 212 schools – which span 12 state universities – by offering free training, hands-on labs and certification opportunities to students. Additionally, Fortinet is committed to training more than 25 educators nationwide, ensuring they develop strong expertise in Fortinet technologies and acquire the necessary skills to effectively teach their students.

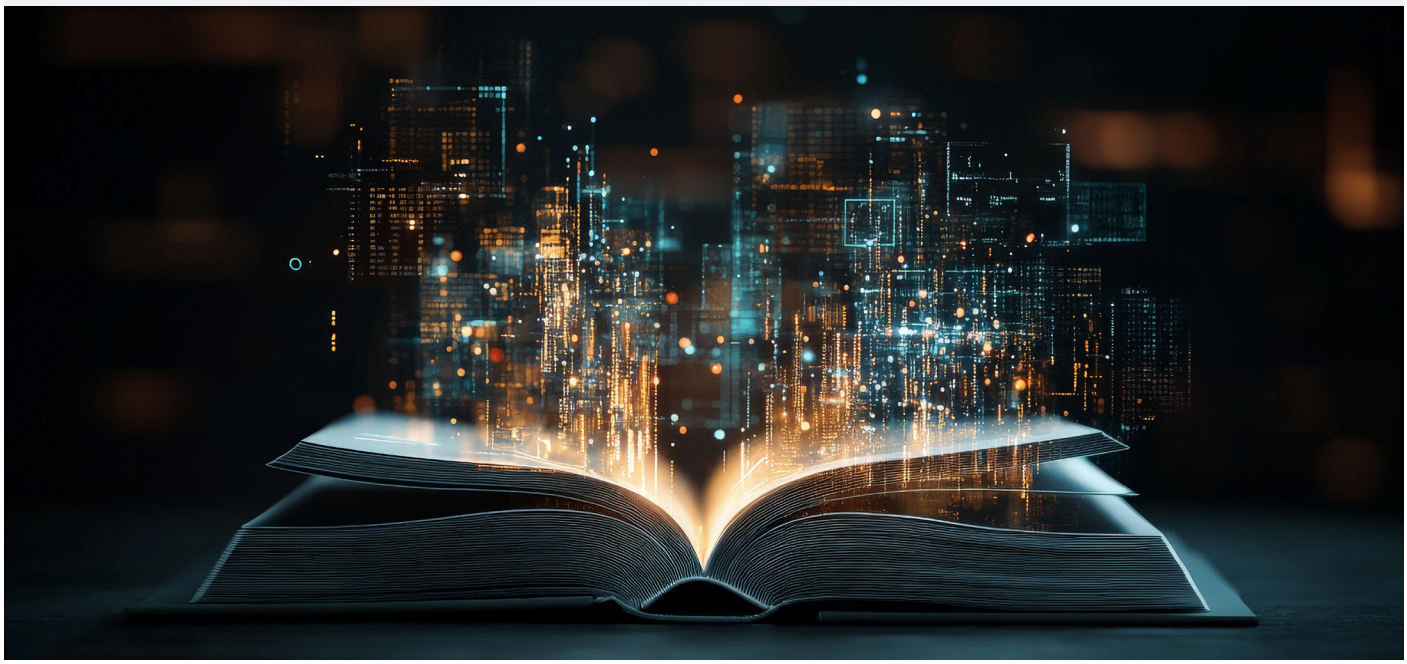
CASE STUDY 10

Banco Santander and Europol

As part of Banco Santander's commitment to law-enforcement collaboration and work towards creating a more secure digital environment, the organization contributes to Europol's annual training event held in Spain for law enforcement officers from multiple nationalities.

During this event, Santander delivers a full day of training covering a range of topics, from quantum cryptography to a workshop on how ATM attacks are carried out. Santander has also provided in-depth, technical, hands-on training sessions. These sessions are tailored to address specific skill-building and emerging threats, covering areas such as digital forensics and cyber intelligence.

The objective of the sessions is to equip Europol personnel with the practical skills and knowledge necessary to effectively investigate and mitigate complex cyberthreats, which will strengthen Europol's capacity to safeguard infrastructure from evolving cyber risks.



Conclusion

If approached strategically, public–private partnerships can be transformative in shaping the next generation of cybersecurity professionals.

As cyberthreats evolve at an unprecedented rate, the demand for skilled cybersecurity professionals continues to outpace supply. Addressing this talent gap is no longer optional: it is a necessity for securing digital assets and networks. PPPs present a powerful solution by combining the strengths of both public and private actors. Private actors contribute agility, expertise and financial resources, while public actors provide policy support, large-scale reach and long-term strategic vision. However, despite their potential, establishing and sustaining these partnerships comes with significant challenges.

Effective collaboration between public and private actors in cybersecurity talent development is often hindered by differences in working speeds, misperceptions of intent and limited access to leading stakeholders. These challenges are compounded by a lack of awareness of local contexts and needs, with global initiatives sometimes overlooking the realities.

While this report is specifically focused on public–private partnerships in the context of cybersecurity, its insights can be valuable for any PPP aimed at tackling the broader topic of talent development.

Successful PPPs depend on bringing together the right stakeholders, maintaining effective project management to ensure that all of the partnership's efforts are aligned with real-world needs and focused on a common objective. For lasting impact, PPPs need to prioritize the creation of sustainable mechanisms such as a training centre that can provide continuous training opportunities.

If approached strategically, PPPs can be transformative in shaping the next generation of cybersecurity professionals. By encouraging strong collaboration, investing in targeted training programmes, cybersecurity challenges or awareness campaigns and ensuring projects are both scalable and sustainable, these partnerships can create a highly skilled workforce equipped to tackle evolving cyberthreats. With the right structure and commitment from all stakeholders, PPPs have the potential to drive long-term change, strengthening global cybersecurity resilience and closing the talent gap.

Contributors

Lead authors

Jael Amponsah Bempah
Project Fellow, Bridging the Cyber Skills Gap, Centre for Cybersecurity

Natasa Perucica
Lead, Capacity Building, Centre for Cybersecurity

World Economic Forum

Tal Goldstein
Head of Strategy and Growth, Centre for Cybersecurity

Akshay Joshi
Head, Centre for Cybersecurity

Acknowledgements

The World Economic Forum extends its gratitude to the members of the Bridging the Cyber Skills Gap initiative for their valuable insights and expertise, shared through a series of workshops and one-on-one interviews. Additionally, the Forum wishes to acknowledge Ariel Nowersztern (Inter-American Development Bank) for his contributions.

Bridging the Cyber Skills Gap initiative

Abdullah Albaiz
National Cybersecurity Authority of Saudi Arabia, Saudi Arabia

Bushra AlBlooshi
Dubai Electronic Security Center (DESC), United Arab Emirates

Ignacio Álvarez Álvarez
Telefónica, Spain

Sagy Bar
Cyber Education Center, Israel

Grant Bourzikas
Cloudflare, USA

Nicole Cader
Absa Group, South Africa

Mariana Cardona Clavijo
Organization of American States, USA

Giuseppe Cinque
Cisco Systems, Italy

Melonia Da Gama
Fortinet, USA

Stefanie Harter
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Germany

Laura Jiménez Orgaz
Banco Santander, Spain

Atul Kumar
Data Security Council of India (DSCI), India

Anat Lewin
World Bank, USA

Vanja Madzgalj
Western Balkans Cyber Capacity Centre, Montenegro

Alberto Martinez Pellicer
Telefónica, Spain

Theoneste Ngiruwonsanga
Smart Africa, Rwanda

Jakub Olszewski
Standard Chartered Bank, Poland

Orhan Osmani
International Telecommunication Union (ITU), Switzerland

Alvin Piket
Trellix, USA

Sarah Powazek
University of California, Berkeley, USA

Thelma Quaye
Smart Africa, Rwanda

Rob Rashotte
Fortinet, USA

Ina Steyn
Absa Group, South Africa

Tara Wisniewski
ISC2, United Kingdom

Production

Bianca Gay-Fulconis
Designer, 1-Pact Edition

Simon Smith
Editor, Astra Content

Endnotes

1. Fortinet. (2024, June). *2024 Cybersecurity skills gap*. https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf
2. Global Cybersecurity Forum and BCG. (2024). *2024 Cybersecurity workforce report: Bridging the workforce shortage and skills gap*. https://web-assets.bcg.com/61/d3/705fbd684d70b0e5f98cdcf7cf47/2024-cybersecurity-workforce-report.pdf
3. ISC2. (2024). *Global cybersecurity workforce prepares for an AI-driven world*. https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf
4. Fortinet. (2024). *Cybersecurity skills gap*. https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf
5. CBRE. (2024). *Cybersecurity: Global talent spotlight*. https://www.cbre.com/insights/viewpoints/cybersecurity-global-talent-spotlight#:~:text=The%20Washington%2C%20D.C.%20metro%20area,fourth%20largest%20for%20cybersecurity%20talent
6. Coursera. (2024). *Global skills report*. https://www.coursera.org/skills-reports/global
7. World Economic Forum. (2025). *Future of jobs report 2025*. https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf
8. Deloitte. (2025). *Nigeria cybersecurity outlook 2025*. https://www.deloitte.com/ng/en/services/risk-advisory/perspectives/Nigerias-cybersecurity-landscape-in-2025.html
9. The term “japa syndrome” refers to a phenomenon in Nigeria where individuals, particularly younger Nigerians, choose to migrate abroad in search of better opportunities, often with little intention of returning home.
10. Gilbert, P. (2024). *Africa faces increased cyberthreats and security skills gap*. Connecting Africa. https://www.connectingafrica.com/skills-and-training/africa-faces-increased-cyberthreats-security-skills-gap-cisco
11. IITPSA. (2024). *IITPSA ICT skills survey*. https://www.iitpsa.org.za/wp-content/uploads/2024/10/2024-IITPSA-ICT-Skills-Survey-and-Research-Report.pdf
12. Tech for Good Institute. (2024). *Using data to protect data: Addressing gaps in cyber threat reporting in the Philippines*. https://techforgoodinstitute.org/blog/expert-opinion/using-data-to-protect-data-addressing-gaps-in-cyber-threat-reporting-in-the-philippines/#:~:text=Philippine%20Cybersecurity%20Capacity&text=An%20upcoming%20Tech%20for%20Good,cybersecurity%20professionals%20in%20the%20country
13. IITPSA. (2024). *IITPSA ICT skills survey*. https://www.iitpsa.org.za/wp-content/uploads/2024/10/2024-IITPSA-ICT-Skills-Survey-and-Research-Report.pdf
14. CBRE. (2024). *Cybersecurity: Global talent spotlight*. https://www.cbre.com/insights/viewpoints/cybersecurity-global-talent-spotlight#:~:text=The%20Washington%2C%20D.C.%20metro%20area,fourth%20largest%20for%20cybersecurity%20talent
15. OECD. (2024). *Building a skilled cyber security workforce in Europe*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/building-a-skilled-cyber-security-workforce-in-europe_6abaf769/3673cd60-en.pdf
16. UNESCO. (2023). *Global education monitoring report, 2023: technology in education: A tool on whose terms?* https://unesdoc.unesco.org/ark:/48223/pf0000385723.locale=en
17. Ibid.
18. Forbes. (2022). *The increasing cost of cybersecurity boot camps*. https://www.forbes.com/consent/ketch/?toURL=https://www.forbes.com/councils/forbestechcouncil/2022/07/29/the-increasing-cost-of-cybersecurity-boot-camps
19. Allianz. (2025). *Allianz Risk Barometer 2025*. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf
20. ISC2. (2023). *Cybersecurity workforce study 2023*. https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf
21. ISC2. (2024). *Women in cybersecurity: Inclusion, advancement and pay equity are keys to attracting and retaining more women*. https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Inclusion-Advancement-Pay-Equity
22. ENISA. (2017). *Public private partnerships (PPP): Cooperative models*. https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-3%203%20Public%20Private%20Partnerships%20%28PPP%29%20Cooperative%20models.pdf
23. Rwanda Inspirer. (2024). *Rwanda: Government, Huawei establish university tech competition*. https://rwandainspirer.com/rwanda-government-huawei-establish-university-tech-competition
24. Road2Cyber. (2024). *Road2Cyber Job Fair*. https://www.road2cyber.eu/job-fair
25. TCS. (2024). *TCS and UK govt create unique cyber policy scholarship for Indian professionals*. https://www.tcs.com/who-we-are/newsroom/press-release/tcs-uk-govt-cyber-policy-scholarship

26. IITPSA. (2024). *IITPSA ICT skills survey*. https://www.iitpsa.org.za/wp-content/uploads/2024/10/2024-IITPSA-ICT-Skills-Survey-and-Research-Report.pdf

27. Fortinet. (2024, June). *2024 Cybersecurity skills gap*. https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf

28. UK Government. (n.d.). *Cybersecurity CNI apprenticeships*. https://www.gov.uk/guidance/cyber-security-cni-apprenticeships

29. Communications Authority of Kenya. (2024). *CA unveils bootcamp and hackathon series ahead of October cybersecurity awareness month*. https://www.ca.go.ke/ca-unveils-bootcamp-and-hackathon-series-ahead-october-cybersecurity-awareness-month-0

30. UK Government. (n.d.). *Work in the UK as a leader in digital technology*. https://www.gov.uk/global-talent-digital-technology

31. ISACA. (2024, October 1). *State of cybersecurity 2024*. https://www.isaca.org/state-of-cybersecurity-2024?utm_source=isaca&utm_medium=other&utm_campaign=cyber-month&utm_term=misc_cybersecurity_awar_isaca_other_behav&utm_content=q3%202024

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org