No. 4 / September 2025
Security Blueprint

Building a Sustainable Cybersecurity Talent Pipeline:

Unlocking the Potential of the German–Philippine Defense Cooperation

Dr. Sven Herpig

Executive Summary

The recently signed Philippine–German Defense Cooperation Agreement includes cybersecurity as a priority area, offering a potential model to address Europe's skills shortage while strengthening the Philippine talent pipeline. Traditional agreements often emphasize information sharing but rarely overcome barriers to intelligence exchange, making structured talent development and institutional cooperation more impactful. Germany brings advanced cybersecurity regulations, sector-specific standards, and experience in emerging technologies, while the Philippines offers a growing cybersecurity workforce, a mature labor migration system, and a strong IT-enabled services sector.

The proposal emphasizes scaling Philippine training to create surplus talent, including by strengthening the early engagement of women and girls in the field, while supported by safeguards against brain drain. Measures include mutual recognition of certifications, dual-degree programs, cyber ranges, apprenticeships modeled on Germany's *Ausbildung*, and structured pathways for professionals to gain international experience before returning home. Public–private partnerships and cybersecurity-focused business process outsourcing (BPO) could expand remote service delivery while strengthening domestic capacity.

By aligning with frameworks such as ENISA's European Cybersecurity Skills Framework, the ASEAN Cybersecurity Cooperation Strategy, and EU CyberNet, the initiative aims to embed international best practices while prioritizing local resilience. If implemented, this approach could serve as a proof of concept for international cooperation, transforming global talent shortages into an opportunity for shared growth, innovation, and collective security.

Introduction

On 15 May this year, it was publicly announced that Germany and the Philippines had signed the Philippine–German Arrangement on Defense Cooperation in Berlin on 14 May.[1] The bilateral framework includes provisions for closer collaboration on cybersecurity, among other areas. The announcement was hardly unexpected: Both countries face one of the most capable and persistent actors in the global cyber domain—the People's Republic of China.[2]

At this stage, the specifics of how the arrangement will be implemented in the field of cybersecurity remain unclear. In many such agreements, "information exchange" is cited as a key area of cooperation. Yet in practice, vague definitions of what such exchanges entail—combined with high thresholds for sharing sensitive threat intelligence—often limit their effectiveness, especially when the partnership is in its early stages. Without clear operational frameworks, such provisions risk remaining aspirational.

Moving beyond information exchange

For both countries, the greatest potential may lie in organizational and institutional cooperation. Germany, home to one of the best-resourced national cybersecurity agencies in Europe, can draw on a wide range of established tools: internationally recognized baseline security catalogues,[3] sector-specific security frameworks, and experience in securing emerging technologies such as artificial intelligence, quantum computing, and next-generation mobile networks (6G). Germany also has significant experience implementing and transposing the European Union's robust cybersecurity legislation.[4]

In return, Germany—and by extension much of the European Union—faces a well-documented shortage of cybersecurity professionals. Estimates suggest that Europe could require up to **500,000 additional specialists** to meet current and near-future demand.[5] This gap is particularly acute in operational cybersecurity roles, incident response, and industrial control systems security.

The Philippines: a skilled workforce with global reach

The Philippines, for its part, has long experience in "exporting" talent. Since the 1970s, it has built a "comprehensive migration management system that can be described as setting the gold standard for migrant-origin countries."[6] By 2023, with deployments recovering from the COVID-19 pandemic, more than two million Filipinos were working overseas, sending home around €3.5 billion in remittances—a vital pillar of the Philippine economy.[7]

The country's strong digital culture is well established. It has a vibrant hacker and security researcher community, visible in events such as the long-running ROOTCON conference.[8] The domestic cybersecurity sector is growing rapidly,[9] supported by an expanding base of certified professionals.[10] Skills development is already on the national policy agenda, with initiatives aimed at producing a workforce capable of meeting domestic demand.[11]

If training programs were scaled to produce more specialists than the local market requires so that it does not undermine domestic needs, **cybersecurity professionals could emerge as a new category of Overseas Filipino Workers (OFWs)**, alongside the traditional roles in health care, maritime services, and IT-enabled business processes.

Why cybersecurity could fit the OFW model

So far, Germany's recruitment of Filipino professionals has focused heavily on the health sector.[12] Cybersecurity, however, offers a promising new avenue. While the colder climate, cultural differences, and bureaucratic hurdles in professional recognition might understandably deter some of the potential candidates,[13] Germany remains attractive in other respects: strong social security provisions, high-quality health care, physical safety, and a stable environment for raising families. For many Filipino professionals, these factors may outweigh the downsides, particularly if deployment is part of a planned career path rather than an open-ended migration.

The certification question

In cybersecurity, professional certifications are often seen as a mixed blessing. Many practitioners view them as helpful for landing interviews but less reflective of actual job performance. However, when the goal is to build a transnational talent pipeline, internationally recognized certifications can be essential. They provide a common standard for validating the knowledge, skills, and abilities of those responsible for securing IT systems and infrastructure. For Filipino professionals working abroad, the absence of formal recognition of qualifications often forces them into lower-level roles. Widely accepted certifications can help ensure that overseas Filipino workers are employed and compensated in line with their actual expertise.

Here, existing international frameworks offer a starting point. Certifications from nonprofit professional associations such as the Information Systems Audit and Control Association (ISACA) and the International Information System Security Certification Consortium (ISC2) are recognized in both countries. Partnering with these organizations could streamline qualification recognition and establish joint training programs, potentially with modules tailored to Germany's regulatory environment and sector-specific security needs.

Mitigating the "cyber brain drain"

Even if the intergovernmental policy framework succeeds and Germany establishes itself as an exemplary host country—for example, by providing clear pathways for career recognition through certifications or equivalent mechanisms—**a major challenge remains: how to manage the potential brain drain of the Philippines' cybersecurity workforce.**[14]

While the Philippine government must improve incentives for skilled professionals to join and remain in public service, **Germany will also carry a responsibility to ensure that its recruitment does not inadvertently weaken the Philippines' state of cybersecurity.** This responsibility stems not only from ethical considerations but also from strategic self-interest: a less cybersecure Philippines could become a more attractive target for malicious actors, creating risks that extend far beyond its borders.[15]

Germany's engagement should combine capacity-building with talent recruitment.[16] This could involve investing in domestic training and education programs, deploying scalable defensive tools—such as security solutions at the Internet Service Provider level—and promoting the exchange of organizational best practices. For information security roles suitable for remote delivery, Germany could collaborate with its private sector to develop cybersecurity-focused business process outsourcing (Cybersecurity BPO) operations in the Philippines. This would allow Filipino professionals to contribute to German and international projects while remaining in-country. Creating an enabling environment for such BPOs would also require addressing persistent challenges, such as unreliable internet connectivity. However, remote work should complement rather than replace other initiatives, as it offers limited opportunities for advancing up the value chain.

By coupling recruitment with sustainable skills development and infrastructure support, Germany can help ensure that international cooperation strengthens, rather than depletes, the cybersecurity posture of its partner nations.

Toward a structured partnership

For the cybersecurity component of the Philippine–German arrangement to deliver tangible results, both sides will need to move quickly from broad statements of intent to structured, measurable programs.

1. Education and talent development

Focus on building a robust, diverse cybersecurity talent pipeline in the Philippines:

- Strengthen early engagement of girls and women through events, internships, stipends, and scholarships to broaden participation.
- Establish undergraduate programs in applied cybersecurity, including advanced fields like Security Operations (SecOps), at public universities.
- Launch a joint dual-degree postgraduate program between the University of the Philippines and a leading German university.
- Invest in cybersecurity laboratories and cyber ranges at key public universities.
- Host joint summer schools on critical domains such as machine learning security or maritime cybersecurity.

2. Applied learning and industry integration

Bridge academic knowledge with real-world practice to strengthen skills:

- Develop a cybersecurity apprenticeship program, modeled on the German *Ausbildung*, linking schools, companies, and the German Chamber of Commerce for recognition.
- Facilitate training exchanges between Germany and the Philippines, focused on high-demand skill areas.
- Offer scholarships for Filipinos to attend global hacking competitions, international conferences, and diplomatic dialogues (e.g., UN-level discussions).
- Support collaborative R&D projects in areas of mutual interest, such as maritime cybersecurity and AI-driven threat detection.

3. Cybersecurity industry growth

Position the Philippines as a trusted regional cybersecurity hub:

- Foster public-private partnerships (PPPs) with German companies to establish Cybersecurity BPOs, backed by improved infrastructure.
- Support an enabling environment for remote security services while emphasizing pathways for professionals to move up the value chain.

4. Talent mobility and migration pathways

Enable international experience while preventing long-term brain drain:

- Negotiate mutual recognition agreements (MRAs) for certifications and work experience.
- Create structured placement programs in Germany with six-month probation periods, supported financially.
- Launch a government employee immersion program where participants work three years in Germany, then return to senior public-sector roles in the Philippines with increased pay.

5. Capacity building and national resilience

Strengthen cybersecurity governance and scalable defensive capabilities:

- Establish a Track 1.5 Germany–Philippines Cybersecurity Dialogue to raise decision-makers' awareness of threats.
- Facilitate exchange of best practices, guidance, and standards between the two countries.
- Collaborate on scalable prevention and detection tooling, especially for critical infrastructure.
- Train cybersecurity experts to become qualified trainers, creating a multiplier effect across the Philippines.

Such a framework would not only address Germany's skills shortage but also help ensure that talent mobility does not come at the expense of the Philippines' cyber resilience. By coupling recruitment with sustained investment in training, infrastructure, and organizational best practices, the partnership could position the Philippines as a significant contributor to global cybersecurity capacity—a role aligned with its long-standing status as a trusted source of skilled overseas professionals.

Anchoring the partnership in the Accra Call's development-first approach,[17] structuring the talent pipeline with the WEF Strategic Cybersecurity Talent Framework,[18] mapping roles and recognition to ENISA's European Cybersecurity Skills Framework (ECSF),[19] and executing with EU CyberNet's[20] coordination and expert networks gives Germany–Philippines cooperation a robust, brain-drain-aware design. By aligning with the ASEAN Cybersecurity Cooperation Strategy 2021–2025,[21] this approach reinforces regional priorities on capacity-building, policy coordination, and trust in cyberspace. Together, these frameworks ensure that local priorities drive the agenda, recognition and apprenticeships open mobility without hollowing out domestic capacity, and scalable defenses, AI-driven threat detection, plus train-the-trainer models deliver scale and sustainability.

If successful, this model could serve as a proof of concept for broader international partnerships in cybersecurity, transforming today's acute talent gap into an opportunity for shared growth, resilience, and collective security.

References

1 Gustavo Guerra, "Germany-Philippines: Defense Cooperation Agreement Signed," *Law Library of Congress,* July 30, 2025, https://www.loc.gov/item/global-legal-monitor/2025-07-30/germany-philippines-defense-cooperation-agreement-signed/.

2 Dr. Sven Herpig, "Cybersicherheit und die Volksrepublik China: Ein Überblick aus deutscher Perspektive," *interface,* November 30, 2021, https://www.interface-eu.org/publications/3183, and for example, Jonathan Greig "China-linked Billbug hackers breached multiple entities in Southeast Asian country," *The Record,* April 23, 2025, https://therecord.media/billbug-china-linked-apt-southeast-asian-country-multiple-orgs-hacked.

3 "IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit," *Bundesamt für Sicherheit in der Informationstechnik,* 2023, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, and "Estonian information security standard (E-ITS)," *Republic of Estonia Information System Authority*, 2024, https://www.ria.ee/en/cyber-security/management-state-information-security-measures/information-security-standard-e-its.

4 Christina Rupp, "Navigating the EU Cybersecurity Policy Ecosystem: A Comprehensive Overview of Legislation, Policies and Actors," *interface*, June 27, 2024, https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem.

5 European Commission "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL – Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience – ('The Cybersecurity Skills Academy')," April 18, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0207.

6 Jeremaiah M. Opiniano and Alvin P. Ang, "The Philippines' Landmark Labor Export and Development Policy Enters the Next Generation," *Migration Information Source,* January 3, 2024, https://www.migrationpolicy.org/article/philippines-migration-next-generation-ofws.

[7] “2023 Overseas Filipino Workrs (Final Results),” *Philippine Statistics Authority,* September 13, 2024, https://psa.gov.ph/statistics/survey/labor-and-employment/survey-overseas-filipinos.

[8] ROOTCON Conference (2025): rc19, https://rootcon.org/html/rc19.

[9] “Cybersecurity – Philippines,” *statista*, June 2025, https://www.statista.com/outlook/tmo/cybersecurity/philippines.

[10] For example ISC2’s “Certified in Cybersecurity” (CC). Data for the Philippines is not publicly available. For an overview over Asia-Pacific, see “2024 Annual Report,” ISC2,August 12, 2025, https://www.isc2.org/insights/2025/08/isc2-2024-annual-report-your-passion-inspires?queryID=03daaecd463eedacf49ed603e8316b5f.

[11] Ludo Fourrage, “Philippines Cybersecurity Job Market: Trends and Growth Areas for 2025,” *nucamp,* February 13, 2025, https://www.nucamp.co/blog/coding-bootcamp-philippines-phl-philippines-cybersecurity-job-market-trends-and-growth-areas-for-2025.

[12] Mary Anne Deveza-Grau, “An Assessment of the International Recruitment of Filipino Nurses to Germany: A Mixed Methods Study,” thesis for the Master of Public Health at the Hamburg University of Applied Sciences, July 25, 2024, https://reposit.haw-hamburg.de/bitstream/20.500.12738/17091/1/MA_Assessment_of_the_International_Recruitment_of_Filipino_Nurses_to_Germany.pdf.

[13] Ibid.

[14] “Coping with cyber brain drain,” *Philippine Daily Inquirer*, June 8, 2024, https://opinion.inquirer.net/174281/coping-with-a-cyber-brain-drain.

[15] TJ Dimacali, “PHL tops global botnet, malware charts –report,” *GMA News*, March 28, 2017, https://www.gmanetwork.com/news/scitech/technology/604985/phl-tops-global-botnet-malware-charts-report/story/.

[16] See for example: EU CyberNet (2025): Enhancing Security Cooperation In and With Asia and the Indo-Pacific (ESIWA+), https://www.eucybernet.eu/project/enhancing-security-cooperation-in-and-with-asia-and-the-indo-pacific-esiwa/.

[17] “Accra Call for Cyber Resilient Development: An Action Framework,” *Global Conference on Cyber Capacity Building,* November 2023, https://gc3b.org/wp-content/uploads/2023/11/GC3B-Accra-Call_Final.pdf.

[18] “Strategic Cybersecurity Talent Framework,” *World Economic Forum White Paper*, April 2024, https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.

[19] “European Cybersecurity Skills Framework (ECSF),” *ENISA*, https://www.enisa.europa.eu/press-office/press-and-media/european-cybersecurity-skills-framework-ecsf.

[20] “Road to International Cyber Capacity Building: Marking 5 Years of EU CyberNet,” *EU CyberNet*, September 30, 2024, https://www.eucybernet.eu/road-to-international-cyber-capacity-building-marking-5-years-of-eu-cybernet/.

[21] “ASEAN CYBERSECURITY COOPERATION STRATEGY (2021-2025),” *ASEAN*, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

The Author

Dr. Sven Herpig is Lead for Cybersecurity Policy and Resilience at the European tech policy think tank interface and a recognized expert on cybersecurity policy in Europe and internationally. He previously held various positions in the German government and worked for the Konrad-Adenauer-Stiftung in Manila (2010–2012), where he also taught at the University of Santo Tomas and Arellano University. He is currently affiliated with the Philippine-based PEERS Consultancy.

On 15 January 2025, Dr. Herpig served as a resource speaker at the KAS Philippines roundtable discussion titled “Bytes and Borders: A Discussion on Germany-Philippines Cyber Defense Cooperation” held in Makati City. This activity marked the first session in a series of forums hosted under the Adenauer Security Experts Network Philippines (SeEN PH) Program. The event explored the key facets of the Germany-Philippines defense arrangement and examined how cyberspace has emerged as a critical domain for strategic cooperation between the two countries.

Imprint

The **Security Blueprint** is a series of policy briefs and short articles addressing critical security issues involving the Philippines and the region from security experts and fellows of the Adenauer Security Experts Network Philippines (SeEN PH) Program.

Disclaimer
The views and opinions expressed by the author do not necessarily reflect the views and opinions of the editorial team and the Konrad-Adenauer-Stiftung. The responsibility for facts, views, and opinions expressed in the article rests exclusively with the author, following that the author may be opinionated and subject to correction and revision.

Publisher
Konrad-Adenauer-Stiftung e.V., 2025, Philippines Office
5/F Cambridge Center Bldg., 108 Tordesillas cor. Gallardo Sts.,
Salcedo Village, Makati City 1227 Philippines
E: info.manila@kas.de
W: kas.de/philippines

Editors
Sophiya Navarro
Daniela Braun

Design and Typesetting
Andreana Chavez

Image Credits
Cover photo created by Andreana Chavez with materials from Unsplash and Wikimedia Commons. Photo of The *Reichstag* building by Jürgen Matern / Wikimedia Commons.