Digital Skills & Jobs Platform

The Weakest Link: Training the EU Workforce to Manage IoT Risks in a Hyperconnected World

Why closing Europe's cybersecurity workforce gap is the missing foundation of IoT security and operational resilience

This paper is part of the Digital Skills & Jobs Platform's Digital Brief 2026 series – a set of deep-dives on key topics in the area of digital skills and frontier technology – produced by some of Europe's leading experts in the field

The DSJP is funded by the Digital Europe Programme of the European Union. Opinions expressed do not necessarily reflect the contracting authority's official position

Table of contents

Tables and Figures

Summary

Across the wider European region, the estimated cybersecurity workforce gap is 424,000 professionals (ISC2, 2024) — and in a world of hyperconnected devices, that gap is no longer just a human resources problem, but a structural vulnerability.

That vulnerability is magnified by the Internet of Things (IoT), which connects physical devices — from industrial sensors and medical equipment to smart meters and consumer products — to networks so that they can exchange data. As these technologies are deployed across critical infrastructure, industrial systems, healthcare, and public services, managing cyber risk depends not only on technical tools, but also on whether organisations have people capable of coordinating across engineering, governance, procurement, and operations under real pressure.

This Digital Brief examines why IoT cybersecurity remains structurally difficult to secure, how workforce fragmentation has become a hidden vulnerability, and what a credible response looks like. Drawing on evidence from the European Union Agency for Cybersecurity (ENISA), IBM X-Force, ISC2, the Organisation for Economic Cooperation and Development (OECD), and NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), it traces the shift from technical protection toward operational resilience —- and argues that building digital skills at scale is the most urgent and most underfunded element of Europe's cybersecurity strategy.

From the Danish energy sector attack of 2023 to the EU's Digital Decade targets and the 2025 Union of Skills strategy, the article connects real-world incidents to policy commitments, workforce data, and practical training approaches —- including simulation exercises and embedded micro-learning —- that are beginning to close the gap between what Europe's regulatory frameworks demand and what its workforce can currently deliver.

Keywords

#IoT cybersecurity, #cybersecurity workforce, #operational resilience, #digital skills, #cyber resilience

About the author

Irina Saavedra is a regulatory technology practitioner and founder with over 15 years of experience across banking, wealth management, and advisory consulting, including positions at Bank of America Merrill Lynch and Bank of Cyprus. Her career has focused on the intersection of financial regulation, operational resilience, and digital transformation — combining deep institutional experience with technical implementation depth across

Salesforce Financial Services Cloud, Data Cloud, and AI. She holds an MBA, and is certified by both Salesforce and IBM in technology implementation. She has contributed feedback to the European Commission's draft guidance on the Cyber Resilience Act (CRA), focusing on implementation pressure points including remote data processing boundaries, third-party dependencies, and cross-framework alignment across CRA, NIS2, and DORA. She is actively engaged with the European Digital SME Alliance and the Shaping Europe's Digital Future initiative. Her published work covers supervisory interpretation and implementation practice across DORA, operational resilience, AI governance, data protection, and regulatory readiness. Irina is the founder of IS-Consulting Services, a regulatory advisory consultancy operating across CEE and DACH markets, and the founder and regulatory model designer of REG-DIGITAL — a deterministic supervisory reasoning model developed in 2025 and validated as an FCA Digital Sandbox participant, preparing for commercial deployment in 2026.

How is Europe's hyperconnected transformation expanding the cybersecurity attack surface?

In May 2023, attackers compromised 22 Danish energy companies in the largest coordinated assault on Danish critical infrastructure to date. The entry point was not a sophisticated zero-day exploit targeting a classified system. It was a firewall — a widely deployed edge device protecting industrial control systems. A patch had been available. Warnings had been issued. The vulnerable devices remained unprotected, and eleven companies were breached simultaneously within hours. Some were forced to disconnect from the national energy grid entirely (SektorCERT, 2023).

The incident illustrates something that statistics alone cannot: **in hyperconnected environments, the weakest link in a security chain is rarely the most technically complex one. It is the neglected one — the unpatched device, the unmapped supplier dependency, the team that received no training in operational technology security.**

Europe's digital transformation is accelerating this challenge at scale. Interconnected ecosystems now link critical infrastructure, public services, cloud platforms, industrial systems, supply chains, and connected consumer technologies. The expansion of IoT environments, Industry 4.0 technologies such as smart manufacturing and industrial automation, and cyber-physical infrastructure is creating new levels of hyperconnectivity. Eurostat data shows that 70% of EU citizens already use IoT devices in their daily lives, while 48% of large European enterprises have deployed connected devices across their operations (Eurostat, 2024).

As these systems become more tightly coupled, the consequences of a single failure propagate further and faster. Operational disruptions, supplier failures, and cyber incidents no longer stay contained — they traverse digital and physical boundaries, affecting manufacturing continuity, transport networks, healthcare delivery, and energy supply simultaneously.

In this environment, cybersecurity is no longer only about protecting individual systems. It is about ensuring that organisations — and the people within them — can continue operating when those systems come under attack.

Why is IoT so structurally difficult to secure?

Despite growing cybersecurity awareness and regulatory attention, IoT environments remain structurally difficult to secure — and the reasons are specific to how these systems are built, deployed, and maintained.

Unlike traditional information technology (IT) systems, IoT environments distribute responsibility across devices, suppliers, cloud platforms, industrial infrastructure, and third-party services without unified visibility or clear ownership. Organisations may struggle to track which devices are connected, identify which suppliers support critical operations, or understand how disruption in one area may affect others. This is not primarily a technical failure — it is an organisational and governance one. As IBM X-Force reports, edge devices such as routers, switches, and virtual private network (VPN) gateways account for more than 75% of all IoT-related cyberattacks precisely because they sit at the boundary between managed and unmanaged environments, often maintained by different teams under different standards (IBM, 2026).

The vulnerability profile of IoT devices compounds this. More than half of known IoT vulnerabilities require no authentication to exploit, meaning attackers can gain remote control of devices without needing stolen credentials or phishing campaigns (IBM, 2026). Many connected and industrial systems remain in service for decades. NIST notes that the lifespan of operational technology systems can exceed 20 years, leaving organisations with hardware or software that is no longer supported and cannot be patched or updated against new vulnerabilities (NIST, 2023).

These dependencies carry real-world consequences. In industrial and operational environments, a cyber incident does not stay digital. Manufacturing for the fifth consecutive year remains the most attacked sector globally, accounting for 27.7% of all monitored incidents (IBM, 2026). In healthcare, 54% of cyberattacks involve ransomware targeting connected medical devices, with each breach causing an average of nineteen days of emergency department disruption (European Commission, 2025). When digital systems are embedded into physical operations, the boundary between a cybersecurity failure and a public safety failure becomes dangerously thin.

As a result, securing IoT environments depends as much on coordination and operational governance as on technical protection — and that dependency places the workforce, not just the technology, at the centre of the problem.

Why is workforce fragmentation becoming IoT security's hidden vulnerability?

Many IoT cybersecurity failures stem not only from technical vulnerabilities, but from the growing difficulty of coordinating security responsibilities across interconnected environments. As cloud platforms, industrial systems, public services, supply chains, and connected devices become increasingly linked, cybersecurity depends on engineering, operations, procurement, compliance, governance, and incident-response teams coordinating effectively during disruption.

The scale of the underlying workforce problem makes this coordination harder than it should be. Across the wider European region, the cybersecurity workforce gap is estimated at 424,000 professionals (ISC2, 2024), while OECD labour-market analysis found demand for cybersecurity professionals growing faster than that of other occupations in the European countries examined (OECD, 2024). Critically, the issue has

shifted from one of headcount to one of capability: 95% of organisations report that skill gaps — not staff numbers alone — directly caused significant security incidents in the past year (ISC2, 2025). Traditional cybersecurity models were designed around isolated technical security teams. Hyperconnected environments have made those models obsolete.

Table 1 — Europe's Cybersecurity Workforce Gap at a Glance

Indicator	Figure	Source
Total EU cybersecurity workforce shortage	300,000–424,000 unfilled roles	ISC2/OECD, 2024–25
OT-specific skills deficit	30,000–45,000 unfilled roles	ISC2, 2025
Organisations where skill gaps caused incidents	95% affected	ISC2, 2025
Current practitioners without formal credentials	76%	European Commission, 2025
Demand growth vs other occupations	Up to 3× faster	OECD, 2024
Women among cybersecurity graduates	Only 20%	OECD, 2024

Sources: ISC2 Cybersecurity Workforce Study 2025; OECD, 2024; European Commission, 2025.

The gap is sharpest in operational technology (OT) environments — the systems controlling physical processes such as industrial machinery, energy grids, and transport networks. Europe's OT cybersecurity skills deficit is estimated at between 30,000 and 45,000 unfilled roles, concentrated in manufacturing, energy, transport, and utilities (ISC2, 2025). These roles are structurally harder to fill than standard IT positions because they require professionals who can bridge two distinct domains: conventional IT security protocols on one side, and legacy industrial control systems — including SCADA (Supervisory Control and Data Acquisition) systems and Industrial Control Systems (ICS), which manage critical physical processes such as power generation, water treatment, and manufacturing automation — physical safety requirements, and operational continuity on the other. An organisation may have a fully staffed IT security team and still be critically exposed because no one on that team has hands-on OT experience.

This fragmentation creates a compounding problem. The rapid enforcement of the NIS2 Directive has expanded mandatory security requirements to thousands of European industrial facilities that previously

had no formal cybersecurity function at all, spiking demand for OT-specific competencies faster than the talent pool can grow (European Commission, 2024). At the same time, 76% of people currently working in European cybersecurity roles hold no formal credentials, and up to 66% transitioned from non-technical backgrounds — meaning the workforce filling these gaps lacks structured preparation (European Commission, 2024).

Recognising this, European frameworks are beginning to redefine what cybersecurity capability means in interconnected environments. The ENISA European Cybersecurity Skills Framework (ECSF), the NIS2 Directive, and the EU Cybersecurity Skills Academy all reflect a shift away from isolated technical expertise toward continuous coordination across governance, engineering, supplier management, and operational resilience. The question is whether workforce development is moving fast enough to match the pace of the threat.

What does operational resilience demand beyond technical cybersecurity skills?

Hyperconnected environments are exposing the limits of cybersecurity models focused primarily on technical protection and incident prevention. The question is no longer only whether an organisation can stop an attack — it is whether it can continue operating when an attack succeeds.

Emerging operational resilience frameworks reflect this shift directly. The most significant recent development is the introduction of the Govern function as the central anchor of NIST Cybersecurity Framework 2.0. Unlike its predecessor, which treated governance as a passive element within the Identify function, CSF 2.0 places governance at the core of the entire framework — requiring executive boards to own cybersecurity as a primary business risk, define organisational risk appetite, and ensure that supply chain dependencies are continuously monitored rather than periodically audited (NIST, 2024). Critically, CSF 2.0 establishes that an organisation is only as resilient as its weakest third-party vendor — a principle that maps directly onto the IoT supply chain vulnerabilities described in the previous sections.

In Europe, the Cyber Resilience Act extends this accountability further, holding manufacturers legally responsible for the cybersecurity of connected products throughout their entire operational lifecycle — not only at the point of sale (European Commission, 2024). Together, these frameworks represent a structural shift from periodic compliance toward Resilience-by-Design: embedding the capacity to absorb, adapt, and recover from disruption into the architecture of systems and organisations from the outset, rather than treating resilience as something added after a crisis (Deloitte, 2023; WEF, 2024).

This transformation is reshaping how organisations evaluate workforce capability. Static certification against a point-in-time standard is no longer sufficient to demonstrate operational readiness. Workforce capability is increasingly assessed through behavioural testing, role-based readiness exercises, simulation analytics, and operational dashboards that measure how individuals and teams perform under pressure — not merely what qualifications they hold. The ENISA European Cybersecurity Skills Framework supports

this shift by defining 12 professional role profiles in terms of their missions, tasks, skills, knowledge, competences, and interdependencies (ENISA, 2022). The WEF reinforces this directly, arguing that technology and processes are operationally useless if the workforce lacks the resolve and situational awareness to act on them (WEF, 2024).

The implication for workforce development is significant: building Europe's IoT cybersecurity capability is not primarily a question of hiring more people with the right certificates. It is a question of how those people are trained to operate.

How can Europe build the IoT cybersecurity workforce it urgently needs?

Expanding the number of cybersecurity professionals is only one part of the solution. The WEF's Global Cybersecurity Outlook states directly that producing more experts will not solve the problem — security capability must be distributed across the entire workforce, not concentrated in a narrow technical team (WEF, 2026). Hyperconnected environments require multidisciplinary operational capability that combines technical expertise with coordination, governance awareness, supplier oversight, and decision-making under pressure. Traditional workforce development models — static training, isolated specialisation, and periodic certification — are not designed to deliver this.

Europe's policy architecture recognises the scale of the challenge. The EU's Digital Decade programme sets a target of 20 million ICT specialists by 2030, with cybersecurity explicitly named as a priority area — yet current projections suggest the EU will reach only 12 million at the present rate of progress (European Commission, 2023). In response, the Union of Skills, published in March 2025, commits the European Commission to accelerating the Cybersecurity Skills Academy and expanding cyber-campus networks across Member States (European Commission, 2025). Since 2021, the Commission has invested approximately €600 million in cybersecurity skills initiatives, with a dedicated €10 million allocation for SMEs and public sector organisations (European Commission, 2025). These commitments sit within the broader framework of the European Pillar of Social Rights, which establishes the right to training and lifelong learning as a foundational principle of fair and well-functioning labour markets — placing IoT cybersecurity workforce development firmly within Europe's social as well as its digital agenda (European Commission, 2021). These are significant commitments — but investment alone does not change how people learn to operate under pressure.

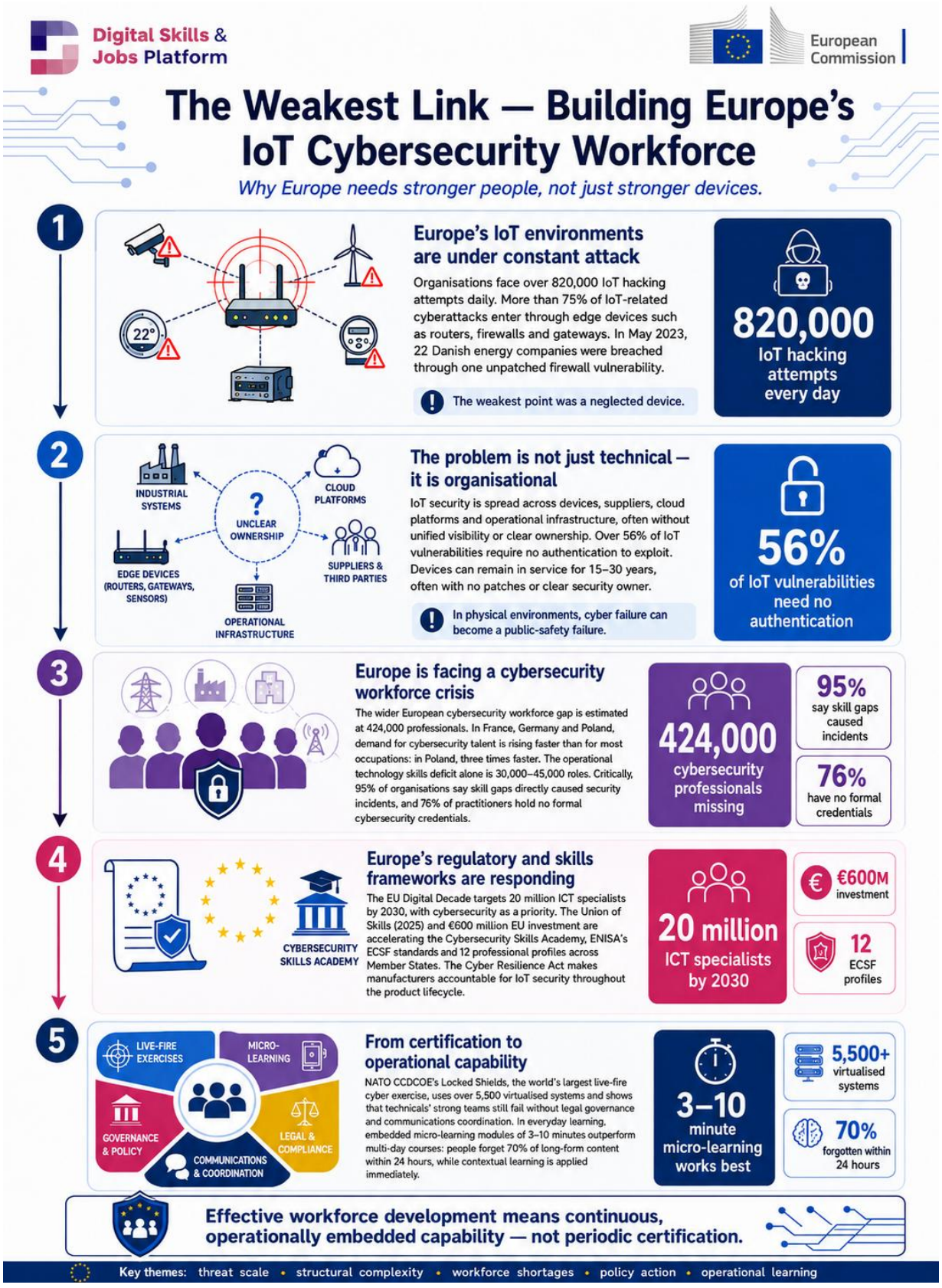
That is why simulation environments are becoming central to workforce development rather than supplementary to it. Exercises such as ENISA's Cyber Europe and NATO CCDCOE's Locked Shields

demonstrate something that classroom training cannot replicate: that operational resilience depends not on individual technical expertise but on the ability of multiple organisational functions to coordinate simultaneously during disruption. In Locked Shields — the world's largest live-fire cyber defence exercise, deploying over 5,500 virtualised systems representing a nation's critical infrastructure — technically proficient teams consistently fail if their legal, communications, or governance functions cannot perform under pressure alongside them (NATO CCDCOE, 2024). The exercise makes explicit what real incidents confirm: a crisis is never only a technical event.

For organisations that cannot run large-scale exercises, embedded micro-learning offers a practical complement. Rather than pulling understaffed teams away from live monitoring for multi-day courses — an operational reality that makes 36% of European security teams unable to access training despite needing it — micro-learning delivers focused three-to-ten minute modules directly within daily workflows, triggered by specific tasks or behaviours (ISC2, 2025). Research consistently shows that people forget up to 70% of long-form training content within 24 hours; contextually delivered, task-specific learning applied immediately is retained significantly longer. European platforms including SoSafe (Germany), Hoxhunt (Finland), and Avatao (Hungary) have operationalised this approach specifically for cybersecurity contexts, integrating behavioural coaching directly into the tools teams already use.

Together, these approaches reflect a broader transformation in workforce development philosophy: from periodic, credential-based training toward continuous, adaptive, and operationally embedded capability building — as reflected in the ENISA European Cybersecurity Skills Framework and the EU Cybersecurity Skills Academy's evolving programme of industry-academic partnerships.

Figure 1. The Weakest Link - Building Europe's IoT Cybersecurity Workforce



Conclusion: From Technical Protection to Capability Resilience

The firewalls that failed in Denmark in 2023 were not the weakest link because they were technically inferior. They were the weakest link because the organisations responsible for them lacked the people, the processes, and the training to keep them secure. That is the underlying condition this article has traced: as IoT environments expand across Europe's critical infrastructure, supply chains, and public services, the limiting factor in cybersecurity resilience is increasingly human and organisational rather than technical. Frameworks, regulations, and investment are aligning — but their value depends entirely on whether Europe can build a workforce capable of operating across interconnected environments under real pressure. In hyperconnected systems, the strength of the chain is only ever as good as the people maintaining it.

Bibliography

Deloitte (2023) *Resilience by design: Financial services operating models and operational resilience*. Available at: https://www.deloitte.com/ca/en/issues/resilience/resilience-by-design.html (Accessed: 15 July 2026).

ENISA (2022) *European Cybersecurity Skills Framework (ECSF) — User Manual*. Heraklion: European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf (Accessed: 15 July 2026).

European Commission (2021) *European Pillar of Social Rights Action Plan*. Brussels: European Commission. Available at: https://commission.europa.eu/publications/european-pillar-social-rights-action-plan_en. (Accessed: 15 July 2026).

European Commission (2023) *Digital Decade Policy Programme 2030*. Brussels: European Commission. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme(Accessed: 15 July 2026).

European Commission (2023) *The EU Cybersecurity Skills Academy Factsheet*. Brussels: European Commission. Available at: https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-skills-academy-factsheet (Accessed: July 2026).

European Commission (2025) *European action plan on the cybersecurity of hospitals and healthcare providers*. Brussels: European Commission. Available at: https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers (Accessed: 15 July 2026).

European Commission (2025) *Union of Skills*. Brussels: European Commission. Available at: https://commission.europa.eu/topics/competitiveness/union-skills_en (Accessed: 15 July 2026).

European Union (2024) *Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (Accessed: July 2026).

Eurostat (2024) Digital economy and society statistics — households and individuals. Luxembourg: European Commission. Available at: https://ec.europa.eu/eurostat/web/digital-economy-and-society (Accessed: May 2026).

IBM (2026) X-Force Threat Intelligence Index 2026. Armonk: IBM Security. Available at: https://www.ibm.com/security/xforce (Accessed: May 2026).

ISC2 (2024) *Building Europe's Cybersecurity Leaders of Tomorrow*. Available at: https://www.isc2.org/Insights/2024/11/Building-Europes-Cybersecurity-Leaders-of-Tomorrow (Accessed: 15 July 2026).

ISC2 (2025) Cybersecurity Workforce Study 2025. Vienna: ISC2. Available at: https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study (Accessed: August 2026).

NATO CCDCOE (2024) Locked Shields 2024 exercise report. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/locked-shields/ (Accessed: May 2026).

NIST (2023) *Guide to Operational Technology (OT) Security*. NIST Special Publication 800-82 Revision 3. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://csrc.nist.gov/pubs/sp/800/82/r3/final (Accessed: July 2026).

NIST (2024) Cybersecurity Framework 2.0. Gaithersburg: National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework (Accessed: May 2026).

OECD (2024) Building a skilled cybersecurity workforce in Europe. Paris: OECD Publishing. Available at: https://www.oecd.org/en/publications/building-a-skilled-cyber-security-workforce-in-europe_3673cd60-en.html (Accessed: August 2026).

SektorCERT (2023) The attack on Danish critical infrastructure. Copenhagen: SektorCERT. Available at: https://cert.europa.eu/publications/threat-intelligence/cb23-12/ (Accessed: May 2026).

WEF (2024) *Unpacking Cyber Resilience*. Geneva: World Economic Forum. Available at: https://www.weforum.org/publications/unpacking-cyber-resilience/ (Accessed: July 2026).

WEF (2026) *Global Cybersecurity Outlook 2026*. Geneva: World Economic Forum. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/ (Accessed: July 2026).