Journal of *Cybersecurity and Privacy*

MDPI

Review

Addressing the Cybersecurity Skills Shortage in Lithuania: Policy Insights from the United Kingdom

Carlene Campbell [1], Sergio Jofre [1], Giedre Sabaliauskaite [2,*], Carolyne Obonyo [1,*] and Odayne Haughton [1]

[1] Human-Environment-Technology (HET) Systems Centre, Mykolas Romeris University, LT-08303 Vilnius, Lithuania; s.jofre@mruni.eu (S.J.)
[2] Faculty of Public Governance and Business, Mykolas Romeris University, LT-08303 Vilnius, Lithuania
* Correspondence: giedre.s@mruni.eu (G.S.); carolyneobonyo@mruni.eu (C.O.)

Abstract

Cybersecurity has become a critical challenge to policy as cyber threats continue to increase in frequency, sophistication, and societal impact, exposing the growing vulnerability of the critical infrastructure supporting vital societal functions. Globally, these risks are heightened by a persistent shortage of skilled cybersecurity professionals, which, in Europe, threatens the effective implementation of the Union's Network and Information Security Directive 2 (NIS2) concerned with the enhancement and harmonization of the cybersecurity level across Member States, notably in terms of their critical infrastructure and involved entities. This article examines the cybersecurity skills landscape across the European Union (EU), with a specific focus on Lithuania, using the United Kingdom (UK) as a strategic benchmark subject. Adopting a comparative case study approach, the study explores and discusses governance arrangements, education and training pathways, labour-market dynamics, and quality-assurance mechanisms shaping cybersecurity workforce development. Technical, organisational, and transversal skills required to prepare an effective cybersecurity workforce in a rapidly evolving labour landscape are also discussed. Findings reveal that Lithuania faces an acute shortage of advanced practitioners and limited alignment between education provision, labour-market needs, and regulatory requirements. In response, the article proposes policy-informed strategies adapted from the UK's structured and professionalised cybersecurity skills model, explicitly mapped to NIS2 workforce and capability requirements. Identified strategies emphasise the need of coordinated action across schools, higher education institutions, government, industry, and the wider community. Potential enablers and constraints for the operationalization of the identified strategies are further analysed and discussed. The study aims to contribute to ongoing policy debates by demonstrating how a strategic context-sensitive selection and adaptation of key components in established skills frameworks can support the development of a sustainable national cybersecurity skills ecosystem and enhance long-term digital resilience, not only in Lithuania but also in other Member States across the EU.

Keywords: cybersecurity skills; cybersecurity governance; workforce capability; regulatory compliance; community of practice; Lithuania

Check for updates

Academic Editors: Martin Gilje Jaatun, Hanan Hindy and Aunshul Rege

Received: 31 December 2025
Revised: 4 February 2026
Accepted: 6 February 2026
Published: 8 February 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

The number and severity of cyber threats have spiralled worldwide, affecting governments, businesses, societies, and the critical infrastructure supporting their functioning.

Increased ransomware campaigns, data breaches, and state-sponsored attacks have intensified the demand for a highly skilled and resilient cybersecurity workforce [1]. However, a global shortage of over 4 million cybersecurity experts evidences a persistent skills gap that poses a significant risk to the national security, economic resilience, and regulatory compliance of nations [2,3]. The challenge is especially pronounced in small EU Member States such as Lithuania, where a limited labour market capacity, higher market sensitiveness to innovation inputs, regional disparities, and strong competition from international employers restrict the development of its workforce [4]. An estimated 63% rise in reported cyber incidents in Lithuania in the 2024–2023 period [5] further underscores the urgent necessity to expand and professionalise the national cybersecurity talent pipeline. Although Lithuania has made considerable progress in cybersecurity governance and education, there are persistent structural gaps in education pathways, professional training, and cross-sector coordination of cybersecurity development skills [1,4,6]. Addressing these challenges has become a strategic imperative, as EU Member States must comply with the NIS2 Directive [7,8], which designates critical infrastructure and essential service operators as critical entities and requires them to maintain dedicated, competent cybersecurity teams with interdisciplinary skills.

This evolving European regulatory landscape has reframed cybersecurity skills from a predominantly technical concern into a strategic, economy-wide policy imperative. Digital transformation and cybersecurity are now embedded into binding EU regulatory and strategic development frameworks, including the NIS2 Directive, the EU Cybersecurity Strategy, the Digital Decade Policy Programme, and the Cyber Resilience Act. In this context, NIS2 explicitly links national cybersecurity capabilities to workforce development, education, and training across an expanded variety of sectors. Complementary initiatives, such as the EU Cybersecurity Skills Academy, the European Cybersecurity Skills Framework (ECSF), and the European Union Agency for Cybersecurity (ENISA), further institutionalise this approach. Consequently, cyber skills are no longer viewed as optional assets but as requirements to regulatory compliance, digital resilience, critical infrastructure protection, and Single Market functioning.

EU Member States retain flexibility in shaping their cybersecurity skills policies and National Cyber Security Strategies (NCSS) in line with domestic priorities, institutional capacity, and labour market conditions. This approach accommodates diverse education systems and industry structures while maintaining alignment with overarching EU objectives, including NIS2 and ENISA's European Cybersecurity Skills Framework (ECSF) [9]—describing twelve basic cybersecurity professional role profiles to create a common understanding between individuals, employers, and learning programmes providers across the EU. However, harmonising national cybersecurity skills strategies with EU frameworks presents Member States with the need to deal with a few shared issues: (a) persistent workforce shortages; (b) mismatches between education provision and industry needs; (c) limited—triple helix—collaboration between academia, industry, and government; (d) constraints to continuously update skills in the face of rapidly evolving threats and technology regimes—e.g., the emergence and rapid ongoing diffusion of transformative and enabling technologies such as Artificial Intelligence (AI) and quantum computing [3,10]. These challenges, particularly acute in states with smaller economies, have been consistently documented in pan-European skills analyses that suggest considerable technical and managerial gaps across key professional roles persist [4].

Such challenges resonate in Lithuania, notably the country's acute shortage of cybersecurity professionals capable of performing multiple ECSF-defined roles and local labour markets struggling to attract and retain experienced, skilled specialists. Recent amendments to the national cybersecurity legislation have increased the demand for designated

cybersecurity personnel [10], adding additional pressure. In this context, we argue, the UK's experience with structured professionalisation, career pathways, and quality-assured training frameworks [1] offers valuable policy lessons, even in the light of insurmountable structural and capacity differences between the two states. However, from a broad strategic contextual perspective, the observation of these mechanisms can provide Lithuanian policymakers with alternative directions when considering how to clarify competency standards, better align university curricula with labour-market needs, and enhance the practical relevance and credibility of cybersecurity training across sectors.

This article examines alternative strategic pathways for developing a cohesive, long-term cybersecurity skills strategy in Lithuania, grounded in national needs and European regulatory obligations. It draws on a comparative analysis of governance, education, labour market, and quality-assurance models, focusing on the UK's structured and professionalised approach to cybersecurity skills development.

By contrasting this model with Lithuania's current policy landscape and institutional capacity, the study identifies and discusses transposable elements such as (a) competency frameworks, (b) professional standards, (c) accreditation systems, and (d) clearly defined career pathways that can be realistically adapted to Lithuania's economic scale, higher-education structure, and SME-dominated labour market. Rather than advocating policy imitation, the study emphasises context-sensitive adaptation to improve alignment between education supply, labour-market demand, and regulatory requirements, including NIS2.

Eventually, the study aims to provide an evidence-informed foundation for strategic decision-making, suggesting a shift from fragmented initiatives toward an integrated, sustainable, and scalable national ecosystem for cybersecurity skills development aligned with long-term digital resilience objectives.

The article is structured as follows. Section 1 introduces the policy context of cybersecurity skills development in Europe, situating Lithuania's challenges within the evolving regulatory framework, notably the context set by NIS2 forthcoming enforcement. Section 2 outlines the methodology, adopting a comparative case study approach to analyse cybersecurity skills ecosystems in the UK, the EU, and Lithuania. Section 3 examines the cybersecurity skills landscape across these contexts, highlighting workforce gaps, institutional arrangements, and labour-market dynamics. Section 4 synthesises the literature on essential cybersecurity skills, encompassing technical, organisational, and soft-skill dimensions. Section 5 discusses the findings, drawing on transferable lessons from the UK to propose policy-informed strategies tailored to Lithuania's economic and institutional context. Finally, Section 6 summarises the key contributions, outlining policy implications and identifying directions for future research, while Section 7 concludes the paper.

2. Methodology

This study employs a comparative case study research design informed by the framework developed by Bartlett and Vavrus [11], which conceptualises comparison as a multi-sited, relational, and context-sensitive analytical process rather than a simple comparison of national models. From this perspective, the UK's and Lithuania's parallels and divergences are interpreted and analysed as a rational set of comparable variables embedded within broader European cybersecurity governance, education, and labour market dynamics. Following horizontal, vertical, and transversal axes of comparison, the study analyses policy frameworks, institutional arrangements, and skills ecosystems across national contexts (horizontal axis), across levels from EU regulation to national implementation and higher education practice (vertical axis), and over time as cybersecurity workforce strategies evolve (transversal axis). In addition to documentary and literature analysis—using Google Scholar Labs engine—the study draws on expert-informed insights gathered from partic-

ipation in national workshops and policy discussions, including CyberHubs Lithuania activities—which are interpreted as situated knowledge reflecting current institutional and stakeholder perspectives. This knowledge is complemented by practice-based evidence derived from the authors' involvement in developing a new university programme in digital technologies and cybersecurity, enabling reflexive analysis of how policy ideas translate into curricular design and institutional constraints. Consistent with Bartlett and Vavrus' methodological framework [11], the aim is not to generalise universally but to produce contextually grounded, policy-relevant insights in which elements of the UK cybersecurity skills model are transferable and adaptable to Lithuania's specific structural, economic, and educational context.

3. Cybersecurity Skills Landscape in the UK, EU, and Lithuania

3.1. The UK's Context

The global cybersecurity workforce is estimated at 5.47 million, with an average annual growth rate of 8% [1]. By comparison, the wider UK cybersecurity workforce—cyber professionals working across sectors—comprises approximately 143,000 professionals, with an annual growth of roughly 5%. The cyber industry—firms providing cybersecurity products and services—employs an estimated 67,300 full-time staff, reflecting a 15% growth over the past year [12,13]. Although recruitment of cyber professionals continues to increase, 49% of the UK businesses report a "basic" skill gap (e.g., setting up firewalls), while 30% indicated a lack of advanced skills such as forensics or cryptography [12]. In 2025, 65% of cyber firms expected an increased need for AI-specific security skills. By the same year, only 17% of the UK cyber workforce was female, against a 48% exhibited by the general workforce [12]. These recent statistics highlight the scale of global demand and the persistent workforce gap facing national labour markets in the UK and abroad.

Yet, the British government has developed a robust cybersecurity ecosystem, underpinned by the establishment of a National Cyber Security Centre (NCSC), which serves as the national technical authority and plays a central role in strengthening cyber resilience [14]. The NCSC provides organisations and individuals with authoritative guidance, incident response support, and workforce awareness initiatives, while also extending its expertise into education and skills development. Through sector-specific guidance and alignment of education standards with industry expectations, the NCSC helps bridge the gap between academic provision and industry requirements, providing unified guidance and supporting standards' development to address labour market shortages, while enhancing graduate employability [14]. Nevertheless, persistent skills shortages remain, and by 2024, approximately 30% of UK cyber firms reported technical skills gaps, particularly in threat detection, secure software development, and incident response [12]. Despite sustained government initiatives, demand for cybersecurity expertise continues to outpace supply [12,13]. The persistent cyber skill gap, not only in the UK but globally, is closely linked to the sustained demand for broad ICT skills across industries and sectors because of an ever faster digital transformation of tasks, processes, functions, and systems [15].

3.1.1. Bridging the UK Cybersecurity Skills Gap

The UK has adopted a coordinated, multi-stakeholder approach to addressing the cybersecurity skills gap (see Figure 1). Led by the NCSC, the approach integrates schools, Higher Education Institutions (HEIs), research, and the private sector into a national collaborative cyber defence ecosystem, providing the strategic direction, quality assurance, and foundational resources to align the efforts of diverse stakeholders towards common national goals. Through this integrated model—the cornerstone of the UK's cyber strategy—

the UK has positioned itself as a global reference in cybersecurity skills development [2,16]. Table 1 summarizes how the Centre operationalises this multi-sector strategy.

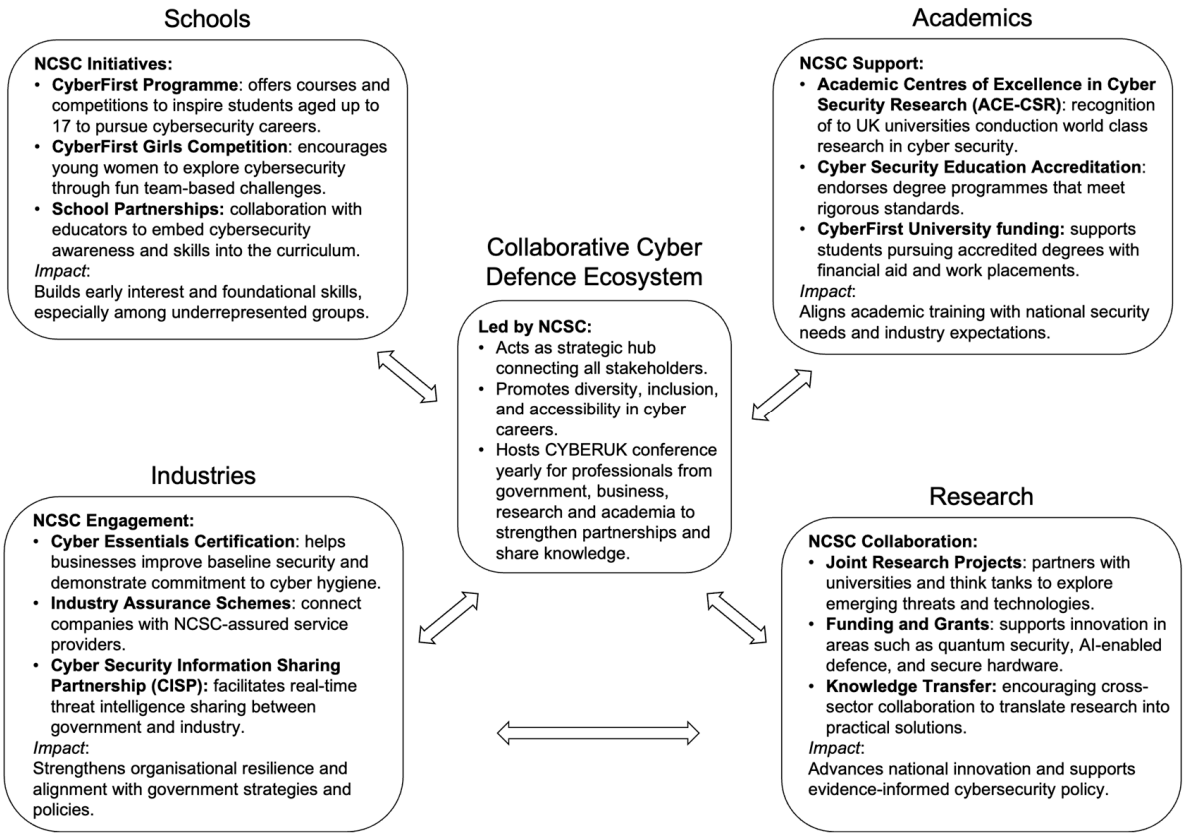


Figure 1. UK's systemic approach to address the cybersecurity skills gap. (source: modified from [14]).

Table 1. The UK's NCSC initiatives across key sectors (source: authors' own sources).

Sectors	NCSC Initiatives	Impact
Schools	CyberFirst, Girls Competition	Early Engagement, Diversity
Academics	ACE-CSR, Certified Degrees	Quality Assurance, Research Excellence
Industries	Cyber Essentials, CISP	Business Resilience, Threat Sharing
Research	Institutes, Transfer projects	Innovation, Academia–Industry Fusion
Cyber Defence Ecosystem	CYBERUK Events & Conference	Coordination, Inclusion, & Dissemination

The Centre collaborates with education providers from schools to universities, supports university–industry partnerships, and engages with industries through initiatives such as "Industry 100" and NCSC for Startups. The research ecosystem is strengthened by virtual research institutes and the safeguarding research infrastructure. Additionally, the Centre established the Cyber Security Body of Knowledge (CyBOK), which informs and underpins cybersecurity education and professional training [17]. In this context, engagement with academics across the education system supports the national talent pipeline by raising awareness, fostering early interest, and aligning educational provision with workforce needs. Initiatives such as the CyberFirst programme [18] were designed to identify and nurture talent from a young age. This programme provides the resources for a range of practical and hands-on activities, including competitions, grants, courses, and summer schools, to foster early interest in cybersecurity. In 2020, approximately

1100 vacancies were offered on residential courses at multiple universities, across levels for ages 14–17.

Another successful product of the ecosystem is the Degree Certification & Academic Centres of Excellence (ACE CSE/ACE CSR) [19], which certifies undergraduate, master's, and apprenticeship programmes, and recognises institutions that achieve excellence in teaching or research in cybersecurity. Similarly, the NCSC Assured Training scheme [20] certifies training providers meeting benchmark standards. For instance, an Open Source Intelligence (OSINT) Practitioner course was approved under this scheme in Wales. The university–industry partnerships actively encourage universities to integrate industry input, reducing the mismatch between graduate skills and employer needs. For example, the University of South Wales [21] emphasises applied learning through "real-world problem-solving with industry collaboration." This is achieved through live briefs, extended work placements, and industry-sponsored research, ensuring graduates are "work-ready."

The ecosystems' support for industries includes the "Industry 100" programme, which invites professionals from industry to work temporarily with the NCSC, fostering a two-way exchange of threat intelligence and practical expertise [22]. This ensures that the NCSC and, by extension, academic partners remain grounded in real-world challenges. Through the NCSC for Startups initiative, innovative startups get connected with technical expertise within the ecosystem to solve national cyber challenges, driving innovation and commercialising research [18]. To reduce cyber risk, the Centre oversees the Cyber Essentials certification, a government-backed minimum standard scheme (simple controls) for organisations [23]. Research is additionally supported by the Vulnerability Research Initiative (VRI) [24], a recent programme that boosts the NCSC's ability to handle evolving vulnerabilities by partnering with external researchers and organisations.

3.1.2. Role of Universities Addressing the Cybersecurity Skills Gap

Several UK universities have developed tailored models to support national efforts on reducing the cybersecurity skills gap, including triple helix collaborations, investing in cybersecurity research, and creating an apprenticeship framework that integrates academic learning with paid workplace experience.

Collaborating with Industry and Government: The University of South Wales developed a partnership with Airbus, BT Group, and the Welsh cyber security cluster to offer an NCSC-certified degree funded by the Welsh Government [21]. In England, Lancaster University leads the CyberFocus regional cluster for the Northwest England region, connecting multiple universities, local authorities, industry players (such as BAE Systems), the Chambers of Commerce, and municipal stakeholders [25]. Similarly, the University of the West of England Bristol (UWE Bristol), holds "gold-level" recognition for cybersecurity education and offers integrated degree apprenticeship routes certified by NCSC, while maintaining partnerships with large employers and government agencies [26].

Investing in Cyber Security Research: The NCSC and the Engineering and Physical Sciences Research Council (EPSRC) can jointly designate universities as Academic Centres of Excellence in Cyber Security Research (ACE-CSR). Designated institutions must demonstrate evidence of sustained investment in cybersecurity research capacity and capability, a critical mass of academic staff engaged in leading-edge cybersecurity research, and a demonstrable record of high-impact outputs [19]. Examples of ACE-CSR universities include the University of Birmingham, University of Bristol, Lancaster University in England, and Cardiff University in Wales.

Creating an Apprenticeship Framework: The UK developed a comprehensive apprenticeship framework, which includes the cyber security apprenticeship programmes, integrating academic learning with paid workplace experience. For example, the University of Wales

Trinity Saint David (UWTSD) has a Digital Degree apprenticeship programme in which students are employed by a company from day one. They spend approximately 80% of their time in the workplace and 20% undertaking university studies one day a week [27]. Hence, participant students can graduate with a full honours' degree and substantial work experience while earning a salary. The university also hosts the Digital Acceleration Programme (DAP)—a twelve-week intensive programme funded by the Welsh Government—to upskill employees of Small and Medium-sized Enterprises (SMEs) in key digital areas. SMEs—the main component in the Welsh economy—often lack the resources for extensive training, but they are increasingly targeted by cyber threats, often lacking enough internal capacity to respond effectively. The DAP programme offers an efficient mechanism for strengthening national cyber resilience by embedding practical skills directly within the workforce [28].

In general, the number of cybersecurity-related apprenticeships in the UK has increased gradually since 2017, from approximately 350 to nearly 4700 in 2024, representing an average annual growth rate of around 40% [5]. Key drivers of this growth include:

1. Expansion of NCSC-accredited apprenticeship and degree programmes (e.g., UWE Bristol, Gloucestershire College);
2. Increased employer participation from large business organisations such as BAE Systems, Airbus, and BT;
3. Integration of work-based learning within academic frameworks, which directly addresses employer skill requirements;
4. Ongoing demand for certified cybersecurity professionals across public and private sectors.

3.2. The EU Context

Rising cybersecurity threats across Europe have intensified the need to address the persistent skills and role gaps within the cybersecurity workforce. In response, the EU has launched various initiatives, including the European Network of Cybersecurity Skills Hubs (CyberHubs) project, seeking to establish a transnational community of practice across Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain. The CyberHubs' skills-needs analysis report on these seven countries identified a mismatch between the cybersecurity skills required and existing education and training provision, "increasing the cybersecurity vulnerability exposure at both the national and European levels" [29] (p. 4). The analysis highlights the need for targeted training strategies, including on-the-job (in-house) training and coaching, recruitment combined with training pathways, and upskilling of existing ICT personnel. Similar studies noted that 74% of companies are not providing dedicated cybersecurity training or awareness activities for their employees. This lack of organisational investment further exacerbates the skills gap by leaving workforces underprepared to manage even basic cyber risks, highlighting the need for more practice-oriented, industry-aligned pathways.

A recent report of the Organisation for Economic Co-operation and Development. (OECD) on "Building a skilled cyber security workforce in Europe" [9] shares insights from three larger EU Member States building national cybersecurity strategies beyond the CyberHubs project—France, Germany, and Poland. In this context, the key aspects of each country's cybersecurity skills strategy reflect distinct labour market trends and education responses. In France, policymakers emphasise diversifying education and training pathways across formal and non-formal programmes and enhancing socio-economic and gender inclusivity, while aligning policy initiatives (e.g., Cyber Campus and SecNumedu initiatives) with industry needs to increase and diversify the cyber workforce. In contrast, Germany prioritises the development of specialised technical and regulatory competencies, with employers demanding expertise in ICT security legislation, standards, and other man-

agerial skills alongside traditional technical capabilities, reflecting the growing industry complexity and evolving nature of the threat landscape. In contrast, the rapid growth in demand in Poland has driven a broader spread of cyber roles and skills into the national labour market, emphasising the need for flexible entry paths and wider experience-based and technical depth in education and training as the ecosystem expands swiftly. These distinctions highlight varied strategic priorities shaped by national economic structures and workforce supply dynamics. However, all three integrate cybersecurity workforce initiatives within EU frameworks (e.g., NIS2 and the Cybersecurity Skills Academy), connecting with networking mechanisms such as the industry-academia Network. These collaborations foster pan-European quality and reciprocity standards for qualifications sharing common resources. However, these strategies—largely federated, voluntary, and project-based alike CyberHubs—are not yet part of institutionally-ratified national frameworks [30,31]. This fragmentation is seen as detrimental for national efforts aimed at identifying and implementing the best-suited strategic model to address local cybersecurity priorities in harmony with EU regulatory directions. However, national institutions are also seen as part of the integration problem—Member States often treat cybersecurity as a sovereign issue, a sensitive national security concern, thus resisting deeper assimilation or sharing mechanisms for workforce development [32].

The European Union Agency for Cybersecurity (ENISA) [8] plays a central role in advancing the cybersecurity community of practice across Europe through sustained collaboration with public and private sector stakeholders. As part of its mandate, ENISA developed the European Cybersecurity Skills Framework (ECSF) to establish a shared understanding of cybersecurity roles, skills, and knowledge. ECSF supports efforts to address skills gaps, align training provision with labour market needs, and promote workforce harmonisation for individuals, employers, and training providers across the EU. ECSF defines the twelve cybersecurity roles required by an organisation, including chief information security officer (CISO); cyber incident responder; cyber legal, policy and compliance officer; cyber threat intelligence specialist; cybersecurity architect; cybersecurity auditor; cybersecurity educator; cybersecurity implementer; cybersecurity researcher; cybersecurity risk manager; digital forensics investigator; and penetration tester [8]. However, for SMEs, with scarcer resources and capabilities, it is challenging—if not impossible—to fulfil these roles. Instead, one cybersecurity professional is expected to perform several roles [4]. In general, the low adoption rate of the ECSF framework denotes persistent inefficacies in the communication among employers, educators, and policymakers [33].

Although roles such as chief CISO, cybersecurity implementer, and cyber incident responder are recognised as critical across the seven Member States, and over 70% of EU companies regard cybersecurity as a high priority, various studies found critical skill gaps and workforce shortages in all three areas, confirming the fact that in Europe as many as 78% of companies declare facing difficulties to recruit qualified professionals [5,29,34]. Without sufficient domestic talent, Member States risk increasing reliance on external providers, creating strategic dependencies that may further undermine long-term autonomy for managing and securing critical digital infrastructure. These constraints are particularly acute in SMEs, which often lack access to qualified cybersecurity specialists and strive to compete with larger organisations for scarce talent [4,33,35].

In general, more than half of European cybersecurity teams are understaffed, due to persistent skills mismatches—with many graduates lacking the hands-on competencies required by employers [34]. Women and minority groups also remain significantly underrepresented across cybersecurity roles, reinforcing structural diversity gaps—over 50% of EU companies do not have any women within their cybersecurity workforce. In addition, a similar proportion of organisations report insufficient dedicated cybersecurity budgets

and that the lack of financial resources increases the pressure on staff, negatively impacting work satisfaction [34]. These factors collectively worsen workforce shortages, constrain workforce capacity, and hinder the development of a resilient cybersecurity ecosystem, thereby exposing the EU to an increased risk of cybersecurity threats.

3.3. Lithuania's Context

Lithuania's cybersecurity strategic framework for the 2023–2030 period is characterized by a centralized governance model designed to counter rapidly evolving hybrid threats in the Baltic region due to shifting unfavourable geopolitical conditions. The Ministry of National Defence (MoD) serves as the lead coordinator through the National Coordination Centre (NCC), shaping national policy and ensuring synchronized action across all related governmental bodies [4,36] (see Figure 2). Operationally, the National Cyber Security Centre (NCSC) functions as the primary agency for unified incident management and the auditing of critical infrastructure [4]. To strengthen military-specific defence, the Lithuanian Cyber Command (LTCYBERCOM) was officially established in January 2025, tasked with planning cyberspace operations and maintaining interoperability with NATO allies [37].

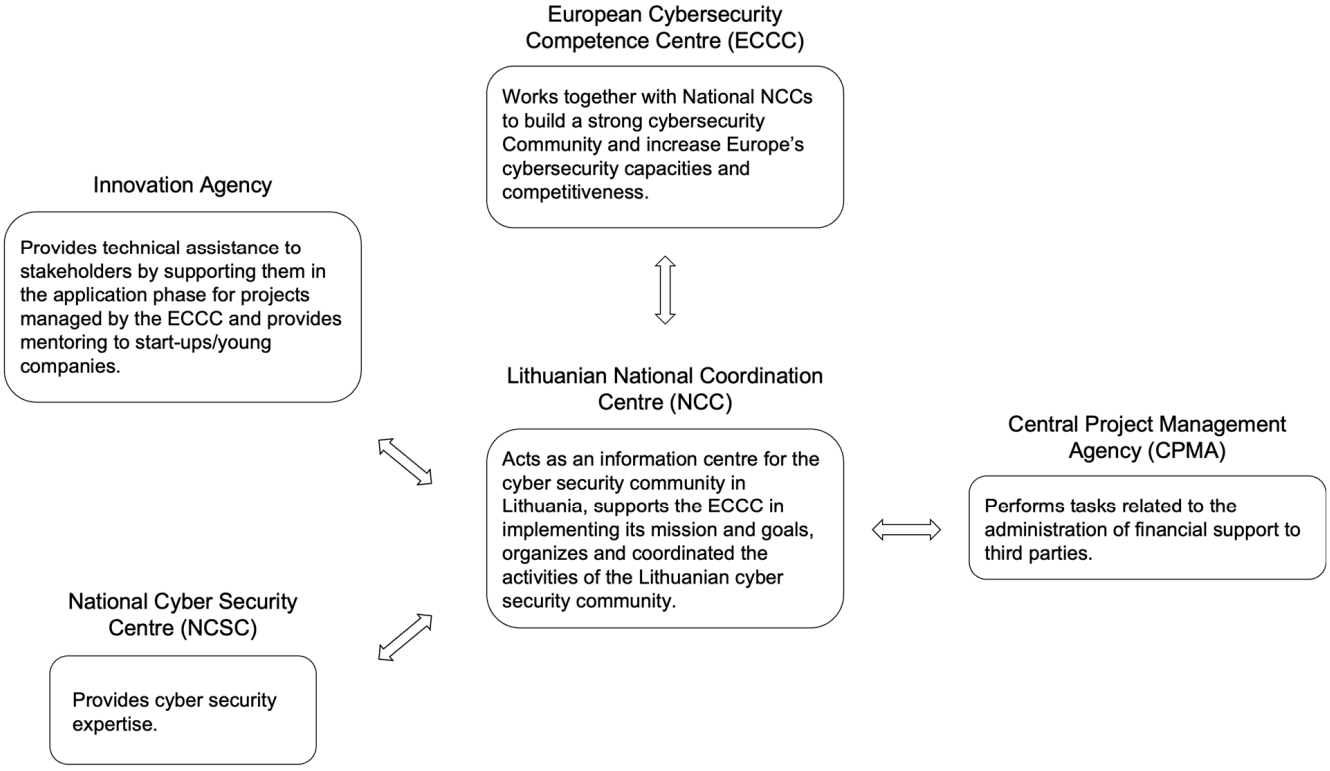


Figure 2. Lithuanian cybersecurity skills governance Framework. (source: modified from [38]).

A core component of the cybersecurity strategy is the National Cyber Security Development Programme, which transposes the European Union's NIS 2 Directive into national law to protect vital digital services. Furthermore, CyberHubs Lithuania—a partnership involving Kaunas University of Technology and industry associations like INFOBALT—addresses the professional skills gap. These hubs foster a collaborative ecosystem between academia and the public sector to develop a specialized workforce and promote innovation in cyber resilience [10].

The demand for certified cybersecurity professionals in Lithuania is expected to more than double over the next 2–3 years [4,10]. Although awareness about the ECSF framework among Lithuanian companies is increasing, the recruitment of personnel without previous formal experience in cybersecurity roles is still a common practice among employers.

In this context, SMEs often seek cybersecurity professionals who can perform multiple cybersecurity-related tasks instead of filling specific roles defined by ENISA's ECSF [8].

A high demand for technical skills in cloud security, data protection, incident management, data analysis, risk management, and policy development/compliance skills [29] limits the country's capacity to detect, respond to, and mitigate cyber threats. Leading organizations need professionals with both technical and soft skills, and with practical experience and certification, instead of newly graduated professionals with only academic qualifications [34]. As indicated in Table 2, Lithuania experiences consistently higher cybersecurity skills shortage compared to the EU average across all assessed domains [5,10,29]. The elevated shortages in incident response (68% vs. 51%), cloud security (62% vs. 44%), threat intelligence (55% vs. 39%), and policy and compliance (48% vs. 33%) underscore the importance of targeted workforce development initiatives aligned with NIS2 requirements.

Table 2. A comparative assessment of cybersecurity skills shortages in Lithuania and the EU (source: authors' own sources).

Cybersecurity Skill Area	Lithuania (%)	EU Average (%)
Incident Response	68	51
Cloud Security	62	44
Threat Intelligence	55	39
Policy & Compliance	48	33

Lithuania also experiences challenges in workforce development and training. Companies do not provide training or implement awareness campaigns about cybersecurity on a regular basis [5], arguing that there is lack of understanding about what kind of training is required [10]. Although four universities in Lithuania offer cybersecurity programmes [1], industry demand exceeds graduate output. Moreover, certain competencies, such as cybersecurity auditing, consulting, and the dissemination of expertise through training, remain underdeveloped at both HEIs and training providers. Current study programmes do not offer core competencies required by employers, highlighting the need to enhance and update the curricula in closer collaboration with industry [10]. In this regard, CyberHubs Lithuania suggests that universities could update study programs matching the specific role profiles defined by ENISA's ECSF framework, while industry associations could facilitate internships and practical training modules in connection to professional certification programmes, integrating international certifications into university degrees to ensure graduates are "market-ready" upon completion. However, as a one-university-led, time-limited project, the CyberHubs strategy, although sensical, risk to remain aspirational rather than operational. Lacking a comprehensive, unified cyber skill strategy aligned with a strongly institutionalized cybersecurity framework, the advancement of cybersecurity research, innovation, education, and training is at risk of further fragmentation [4].

Table 3 compares the cybersecurity skills situation in the UK, EU, and Lithuania with respect to strategic scope, governance and institutional mechanisms, profession and career pathways, education and training quality assurance, labour market and industry alignment, SME and broader workforce, EU regulatory alignment, and long-term continuity.

Table 3. Comparative Overview of Cybersecurity Skills Strategies and Governance Frameworks (source: authors' own sources).

Policy Dimension	UK Cybersecurity Skills Strategy [39,40]	European Network of Cybersecurity Skills Hubs (CyberHubs) [29]	Lithuanian CyberHubs National Strategy [10]	Lithuanian National Policies & Programmes [41,42]
Strategic Scope	Embedded in the National Cyber Strategy, covers the entire talent pipeline, addressing skills gap, professional excellence, and cyber hygiene across all sectors.	Collaborative network of 7 national cybersecurity skills hubs bringing talent gap, enhance professional training, & foster innovation.	Building highly skilled, adaptable cybersecurity workforce, integrating ENISA's ECSF roles (e.g., CISO)	National Digital Decade roadmap sets broad digital skills goals; National Coordination Centre (NCC) coordinates cybersecurity ecosystem under EU competence frameworks.
Governance & Institutional Mechanisms	UK Cyber Security Council provides ongoing professional coordination; UK NCSC runs training assurance & partner programmes.	Project-based network with stakeholder coordination, establishing collaborative hubs nationwide.	Involves national stakeholders (industry, academia, public sector) & works with National Cybersecurity Centre (NCSC) to align strategy (local governance and action planning).	The Ministry of National Defence's NCC, organizes and coordinates activities of the cybersecurity community with EU frameworks. Coordinates work with Innovation Agency Lithuania, NCSC, & Central Project Management Agency (CPMA)
Profession & Career Pathways	Comprehensive career frameworks with defined roles, competencies, & professional standards for cybersecurity careers.	Provides skills gap analyses & recommendations, but no formal career/professional registers.	Identify the need for versatile specialists (skill on at least 3 ENISA's ECSF roles) & emphasises collaboration to tailor training. No formal unified career framework is yet available.	Current national policies do not yet provide detailed professional pathways; emphasis remains on ICT skills improvement and ecosystem coordination.
Education & Training Quality Assurance (QA)	UK's NCSC Assured Training benchmarks training quality to ensure relevance to market and regulatory needs.	Recommends stronger coordination between education, industry & government but does not establish national QA schemes itself.	Calls for modernised training programmes & practical skills development with international certification opportunities but lacks national assurance mechanisms.	National education policies support general digital skills development but lack specific assurance frameworks for cybersecurity training quality as per industry requirements.

Table 3. *Cont.*

Policy Dimension	UK Cybersecurity Skills Strategy [39,40]	European Network of Cybersecurity Skills Hubs (CyberHubs) [29]	Lithuanian CyberHubs National Strategy [10]	Lithuanian National Policies & Programmes [41,42]
Labour Market & Industry Alignment	Focus on aligning skills with employer needs and labour market demand, bridging education outputs with workplace roles. Yet skills shortages & recruitment issues persist.	Include recommendations to involve industry and close skills gaps, but implementation mechanisms remain largely voluntary.	Highlights employer demand for diverse competencies (technical & non-technical), emphasising collaboration to improve training relevance.	National labour and digital policies acknowledge shortages in cybersecurity specialists and aim to integrate skills development programs, but actionable measures are emerging.
SME & Broader Workforce Focus	UK standards and frameworks assist SMEs in recognising skills and training requirements, improving hiring process and compliance readiness.	EU strategies recognise SME involvement but lack direct incentives or simplified tools targeted specifically at SME constraints.	Acknowledges SMEs' needs implicitly via training & awareness actions but does not yet provide dedicated SME-oriented mechanisms.	National ecosystem initiatives support SMEs' cybersecurity needs, but programmes are at an early stage of development.
EU Regulatory Alignment (e.g., NIS2/ENISA)	As post-Brexit (in 2020), the strategy does not directly address EU programs/regulations, but aligns with best practices and global standards, where NIS2 & ENISA principles might be indirectly addressed.	Explicitly designed for EU alignment with NIS2 & ENISA's ECSF coordinated frameworks across Member States.	Explicitly integrates NIS2 & ENISA role expectations into competency gap analysis and training priorities.	National digital and cybersecurity policies are framed within EU Digital Decade and NIS2 regulatory frameworks, emphasizing compliance and ecosystem readiness.
Long-Term Continuity	Institutionalised bodies (Cyber Security Council, NCSC programmes) ensure continuous policy updates and implementation beyond project cycles.	Funded as a time-limited Erasmus+ project; long-term sustainability depends on national adoption beyond April 2027.	Needs national institutionalisation to ensure sustainability beyond the project timeframe; current strategy establishes foundations but not permanent structures.	National programmes such as NCC and Digital Decade commitments provide some continuity, but cybersecurity skills governance is still underdeveloped.

4. Essential Skills for Cybersecurity Professionals

The effectiveness of a national cybersecurity expert and workforce does not only depend on the number of available professionals for these roles but also on the breadth, depth, and integration of the skills provided. Modern cybersecurity roles require a combination of a wide range of abilities, including technical skills, organisation-related skills, and soft skills [29].

4.1. Technical Skills

Technical competence forms the foundation for cybersecurity expertise, which is the most visible skills gap across Europe. Cybersecurity professionals must master technical domains such as network security, cryptography, penetration testing, cloud security, malware analysis, and incident response [29]. Organisations are increasingly migrating to cloud-based infrastructures and adopting DevOps practices, both of which expand the attack surface and expose these environments to persistent adversarial activity. As a result, the demand for continuous monitoring and proactive security measures is intensifying. Currently, employers are seeking advanced expertise in AI-driven threat detection, automated incident response, data-driven security analytics, and secure DevOps practices to safeguard these rapidly evolving digital ecosystems. Without these capabilities, organisations face considerable challenges to detect, contain, and recover from cyber incidents promptly [43].

Countries such as Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain are in high demand for incident management, access control, threat analysis, cloud security, data privacy, and cryptography [10]. These reflect the operational realities faced by organisations subject to increasing cyber threats and regulatory scrutiny. In addition, organisations in these Member States also report persistent shortages in key IT-related skills such as data analysis, system administration and integration, network management, operating systems (OS) security, software development and computer languages, and architecture & infrastructure design. This highlights a structural challenge where cybersecurity professionals are increasingly expected to combine traditional IT competencies with specialised security expertise, particularly in SME environments where roles are consolidated rather than specialised [29].

4.2. Organisation-Related Skills

Organisation-related skills are essential for translating technical security measures into coherent organisational resilience. They include project management, risk management, strategic planning, and policy development [29]. As cybersecurity increasingly becomes a board-level concern, professionals must be able to align security initiatives with organisational objectives, regulatory requirements, and risk appetites. In the Lithuanian and wider EU context, organisation-related skills are important due to the regulatory implications of frameworks such as GDPR and the NIS2 Directive [7], which impose accountability on organisations rather than solely on technical teams. Cybersecurity professionals must therefore contribute to risk assessments, compliance reporting, incident governance, and business continuity planning. However, studies indicate that many cybersecurity practitioners are promoted into governance roles without sufficient training in organisational strategy or policy development, leading to gaps between technical controls and executive decision-making [29]. Strengthening organisation-related competencies through targeted education and professional development is therefore essential to ensure that cybersecurity functions operate effectively at both technical and managerial levels [44].

4.3. Soft Skills

In addition to technical and organisational expertise, soft skills have emerged as strategic requirements for cybersecurity professionals [45]. Cybersecurity is inherently cross-functional, requiring collaboration between IT teams, legal departments, executive leadership, regulators, and external partners. Consequently, communication, problem-solving, teamwork, project management, leadership, and critical thinking have become core competencies in cybersecurity roles, often outweighing narrow technical specialisation in senior positions [34]. These capabilities also underpin ethical judgement and risk-based

decision-making, enabling professionals to navigate complex organisational, regulatory, and operational constraints with confidence and accountability [44].

Effective communication is a critical competency, enabling cybersecurity professionals to translate complex technical risks into clear, actionable insights for non-technical stakeholders [44]. Equally, teamwork and cross-departmental collaboration are indispensable during incident response, where the speed and coherence of coordinated action directly influence the success of containment and recovery efforts. Adaptability has also become increasingly important as threat landscapes and technologies change rapidly, requiring continuous upskilling and the capacity to respond to emerging attack vectors. Ethical judgment and risk-based decision-making are also essential, particularly when navigating privacy considerations, regulatory requirements, and legal constraints in roles such as Cybersecurity Policy Advisor, Awareness Officer, and Governance Analyst [29,34]. In the absence of these soft skills, technical expertise alone is insufficient to deliver effective and sustainable cybersecurity outcomes [45].

4.4. Other Important Qualities

Beyond technical competencies, high-performing cybersecurity professionals exhibit personal, interpersonal, and professional attributes essential for sustained effectiveness in complex threat environments. These include a continuous learning mindset, ethical behaviour, resilience under pressure, and cross-sector fluency. Continuous learning is critical, as cybersecurity knowledge rapidly becomes obsolete, requiring ongoing training and certification to remain aligned not only with evolving threats but also with best practices [46]. In addition, resilience, sound and ethical decision-making under pressure distinguish effective practitioners, while cross-sector fluency enables tailored risk assessment and mitigation across domains. The ECSF supports assessment of these attributes across defined proficiency levels as indicated in Table 4 [8,46].

Table 4. ECSF proficiency levels (source: modified from [46]).

Level	Name	Description
5	Expert	Advises others, handles complex scenarios
4	Advanced	Operates independently in difficult situations
3	Intermediate	Requires occasional guidance
2	Basic	Needs frequent guidance
1	Awareness	Requires close supervision

Within the EU, the nature of cybersecurity competences is multilevel. While technical skills remain most critical, non-technical competencies collectively account for more than half of overall cybersecurity capabilities. This pattern reinforces the ECSF approach, which defines cybersecurity roles through an integrated combination of knowledge, skills, and professional attributes rather than by narrow technical specialisation alone. This raises important questions about the current approach to curricular design in the cybersecurity field, where technical competencies remain dominant [44,45]. Therefore, finding the right balance of skills while keeping curricula as flexible as possible remains a work in progress.

5. Strengthening Lithuania's Cybersecurity Skills Ecosystem: Transferable Lessons from the United Kingdom

Lithuania's need for a coherent, long-term cyber skills strategy has become increasingly pressing due to its rapid digital transformation, heightened exposure to hybrid and cyber threats, and expanding regulatory obligations at both national and European levels. The

implementation of the EU NIS2 Directive significantly extends the range of entities required to manage cybersecurity risks and demonstrate regulatory compliance, thereby placing new workforce demands not only on large operators of critical infrastructure but also on SMEs embedded within digital supply chains [47,48]. In Lithuania, where the economic structure is characterised by a predominance of SMEs and a relatively limited pool of specialised ICT professionals, these developments expose structural weaknesses in the existing cyber skills pipeline, systems of professional recognition, and mechanisms for coordination between education, industry, and government. Comparative evidence indicates that countries with more mature cybersecurity workforce systems rely not solely on expanding training provision, but also on institutional arrangements that structure professional roles, assure quality, and sustain stable talent pipelines [49].

Arguably, the UK represents one of the most developed European examples of such a systemic approach. Rather than framing cybersecurity skills as a purely educational concern, the UK's strategy integrates professionalisation, cross-sector governance coordination, quality assurance, and early-stage talent development within a national strategy that links economic competitiveness, national security, and workforce planning [49,50]. While Lithuania's economic scale, institutional capacity, and higher education landscape differ markedly from those in the UK, several elements of the British model are functionally transferable and could provide an alternative foundation for Lithuanian policy development. In this context, four dimensions merit attention:

(1) Structured professional career frameworks;
(2) Institutionalised multi-stakeholder governance bodies;
(3) National training quality assurance mechanisms; and
(4) Integrated youth and education pipelines.

We argue that addressing these areas would support a transition from fragmented initiatives towards a more coherent cybersecurity skills ecosystem, aligned with European frameworks while remaining responsive to domestic constraints (see Table 3).

5.1. Structured Professional Career Frameworks with Recognised Titles and Certifications

A persistent challenge across Europe is the absence of clear professional identity and role standardisation within the cybersecurity domain, which complicates recruitment processes, education planning, and career mobility [49,51]. The UK has sought to address this issue through a structured approach to professionalisation, led by the UK Cyber Security Council, which develops professional standards, recognised titles (such as Chartered pathways), and competency frameworks grounded in industry practice [50]. This system clarifies expectations regarding knowledge, skills, and experience at different career stages, while providing labour market signals that benefit employers, practitioners, and educators alike.

In the Lithuanian context, such a framework would be particularly valuable given the small size of the labour market and the high degree of role fluidity, especially within SMEs, where individuals frequently perform multiple security-related functions. At present, Lithuanian employers often rely on vendor-specific certifications or informal indicators of experience, which can result in misalignment between qualifications and operational requirements. The adoption of a nationally adapted competency and career framework, aligned with European instruments such as the European Cybersecurity Skills Framework (ECSF) but operationalised through recognised national titles, could enhance transparency, support labour mobility, and strengthen the capacity to meet compliance related roles arising from NIS2 [47,51].

The operationalisation of these strategic elements in Lithuania would entail:

- Mapping national labour market roles against ECSF and UK-based professional standards;

- Establishing voluntary—but formally recognized—professional designations supported by industry associations and HEIs;
- Linking these standards to public sector procurement and regulatory expectations, thereby encouraging employers to value structured competencies.

Potential constraints include limited professional body capacity and the fragmented nature of Lithuania's ICT sector. Nonetheless, a phased approach—initially focusing on critical roles such as Chief Information Security Officers (CISOs), incident responders, and security auditors—would enable early impact while remaining proportionate to national resource limitations.

5.2. Governance Bodies Institutionalising Multi-Stakeholder Coordination

Effective cybersecurity skills policy requires sustained coordination across education, labour, economic development, and national security domains, yet in many countries these areas remain institutionally siloed. The UK addresses this challenge through dedicated coordination structures that bring together government, industry, academia, and professional organisations, with the UK Cyber Security Council and the National Cyber Security Centre (NCSC) fulfilling central convening functions [49].

At present, the country exhibits emerging collaborative platforms, including initiatives under CyberHubs Lithuania, however, implementation and coordination remain largely project-based rather than formally institutionalized [49]. Given that NIS2 places explicit obligations on Member States to ensure adequate national cybersecurity capacity, permanent (or at least long-term) governance arrangements are required to align regulatory demands with workforce planning in the country [47]. The establishment of a permanent, independent, self-regulatory professional body akin to the UK Cyber Security Council—established to define, promote, and uphold professional standards—could integrate and consolidate responsibilities currently dispersed across ministries, agencies, and educational institutions. Such a body could:

- Conduct regular skills needs assessments linked to national risk profiles and regulatory developments;
- Facilitate structured dialogue between SMEs and education providers to ensure training reflects operational realities;
- Coordinate funding priorities across EU and national programmes;
- Support the recognition of professional standards and training quality labels.

Although administrative fragmentation and limited policy capacity present challenges, Lithuania's relatively small scale may also enable more agile governance, provided mandates are clearly defined. Embedding such a body within existing national cybersecurity governance structures, rather than establishing an entirely new agency, could further reduce costs and enhance institutional legitimacy.

5.3. Training Quality Assurance Schemes Linked to National Benchmarks

A recurring weakness in the cybersecurity training market is variability in quality and uncertainty regarding labour market relevance, which undermines confidence among both learners and employers [49]. In the UK, NCSC assured training and academic certification schemes address this issue by benchmarking programmes against nationally defined criteria developed in collaboration with industry [52]. These quality labels serve as credible signals that training provision meets recognised professional and operational standards.

In Lithuania, higher education institutions are expanding digital and cybersecurity programmes, yet employers continue to report deficiencies in practical competencies and regulatory knowledge. The introduction of a national cybersecurity training quality label, aligned with European frameworks (informed by UK and other European countries'

experience), could help to bridge this gap. Such a scheme could encompass university degrees, vocational education, and professional short courses (under a cohesive micro-credential mechanism). Key implementation steps would include:

- Defining competency benchmarks linked to ECSF roles and national regulatory requirements;
- Involving industry practitioners in accreditation and review panels;
- Providing incentives, such as eligibility for public funding or preferential recognition in procurement processes, for programmes that obtain the label.

While resource constraints and accreditation workload may pose difficulties, particularly for smaller providers, shared evaluation frameworks and regional cooperation—potentially at the Baltic level—could mitigate these pressures. Over time, such mechanisms would strengthen the domestic and international credibility of Lithuanian cybersecurity education.

5.4. Youth Pipeline and Talent Engagement Structures Integrated with Formal Education

Long-term resilience in cybersecurity depends on the early and sustained engagement of young people in relevant educational and career pathways. The UK has invested extensively in school-level programmes, competitions, and outreach initiatives that link early talent identification (and nurturing) to higher education and industry opportunities, thereby expanding participation while addressing diversity challenges [49]. In this regard, Lithuania faces demographic decline and a continued outward migration of ICT talent, making the development of domestic pipelines particularly critical—and challenging. Although initiatives promoting coding and digital literacy are in place, cybersecurity remains a niche specialisation that is often introduced relatively late in the education system. Integrating cybersecurity awareness and foundational skills into secondary education, supported by targeted teacher training and partnerships with universities (currently an emerging topic of debate on cybersecurity forums), would help broaden participation and reduce reliance on mid-career reskilling alone. In this context, a few operational measures could include:

- National cyber challenges and extracurricular clubs linked to universities and industry mentors;
- Scholarship schemes aligned with national workforce priorities;
- Clearly articulated school-to-university pathways connected to recognised professional standards.

Still, implementing these actions might present various challenges. In this regard, limited teacher capacity and curriculum congestion are likely to persist; however, modular extracurricular formats and the introduction of digital delivery platforms could help to address these constraints properly. Crucially, linking youth engagement initiatives to visible and credible career frameworks would enhance motivation and reinforce the social recognition of cybersecurity professions. In Lithuania, and arguable elsewhere, the debate on cyber skills should be part of a wider deliberation: how to foster interest and vocation for technical fields, not from siloed disciplinary perspectives but as a wider, attractive professional path with ample applications that requires new interdisciplinary foundations and novel entry and development opportunities.

5.5. Cross-Cutting Considerations: SMEs, Regulation, Economic Structure, and Inclusion

Lithuania's SME dominated economic structure shapes the feasibility and impact of all four policy areas. SMEs often lack the resources to employ highly specialised staff, necessitating policy approaches that support multi-role professionals, shared services, and flexible training pathways. Professional frameworks should therefore incorporate role profiles suited to smaller organisations, while quality-assured short courses and micro cre-

dentials can provide accessible routes for upskilling. On the other hand, regulatory drivers such as NIS2 further increase demand for demonstrable competencies in risk management and compliance, reinforcing the importance of recognised standards and coordinated governance [47]. At the same time, compliance costs may disproportionately affect SMEs, underscoring the need for state-supported training initiatives and clear, accessible guidance.

In the context of inclusion and representation, the UK model underscores the importance of widening participation as a means of expanding and sustaining the talent pipeline. Research indicates a persistent gender imbalance across EU Member States [34], reflecting a structural challenge that limits the sector's overall capacity. Although the UK faces similar disparities, initiatives such as the CyberFirst Girls Competition and the integration of gender inclusive principles within national cybersecurity workforce policy demonstrate how targeted interventions can begin to address this imbalance. For Lithuania, national initiatives promoting inclusive participation—such as targeted scholarships, outreach programmes, and incentives for employers to adopt inclusive recruitment and progression pathways—would certainly help to address cybersecurity skills shortages.

6. Discussion

The evidence synthesised in this review shows that Lithuania's cyber-skills challenge is not merely a question of absolute numbers but of system design: fragmented provision, variable quality assurance, and weak progression routes between education, training, and work experience impede a sustainable talent pipeline [3,4]. While EU initiatives—ECSF, the Cybersecurity Skills Academy, and NIS2—create a shared language and stronger demand signals, they do not in themselves guarantee consistent domestic implementation. Instead, they heighten the emergence of a premium on national coordination, labour market signalling, and quality control across providers [8,33,47]. In this regard, Lithuania mirrors patterns observed across the EU: undersupply of advanced practitioners, shallow hands-on competence among graduates, and SMEs' difficulty in recruiting multi-role professionals [2,9,10].

6.1. What the UK Case Contributes—and What It Does Not

The UK model contributes three policy virtues relevant to Lithuania: (a) institutionalised coordination (NCSC as technical authority and UK Cyber Security Council for professionalisation), (b) assurance mechanisms spanning degrees and short courses (NCSC certification and assured training), and (c) structured pathways from school to doctoral and work-based learning (CyberFirst, apprenticeships, ACE-CSR). Together, these reduce information and communication asymmetries for learners and employers, align curricula with operational practice, and strengthen graduate employability [12,49,52]. However, in this context, transferability is selective, not comprehensive. The UK's scale, funding streams, and institutional density cannot be replicated directly. For Lithuania, the most actionable elements are those that standardise expectations and de-risk employer engagement: clearly defined role/competency frameworks; an assured-training label for short courses; and modular work-based education for SMEs [9,14].

From a different angle, the difference in scales between the UK and Lithuania also raises the issue of whether alternative strategies, such as for example the use of technology as a mechanism to reduce workforce shortages is applicable to the context of this article. As a governance strategy, the UK model does not directly refer to technology-driven mechanisms to reduce technical skills gaps, such as those in ICT in general and Cybersecurity in particular. Literature suggests that by automating routine tasks, improving threat detection, and enabling secure Internet of Things (IoT) platforms using transformative and enabling technologies such as AI and blockchain, persistent skills gaps can be effectively reduced,

easing hiring pressure [53–56]. Contrarily, it is argued that such use of technologies also demands advanced skills themselves, possibly increasing pressure on HEIs to update curricula and on firms, notably SMEs, to invest in additional training [56]. Yet, in a simple rationalization of this ambiguity within the context of our study, one can argue that even if the UK' model would directly consider labour replacement by technology (a.k.a. "technological unemployment") as an object or outcome of its strategy, its transposition in the Lithuanian economic context will be certainly challenging due to constrained investments in automation, and lack of a strong, endogenous innovation system capable to produce the required technological solutions locally.

6.2. Aligning NIS2 Compliance with Workforce Policy

NIS2 reframes cyber skills as a compliance necessity rather than a discretionary enhancement—especially for critical entities, and by extension their supply chains [47]. Lithuania's reported rise in incidents and the extended scope of designated entities intensify demand for expertise in incident response, cloud security, threat intelligence, and regulatory compliance—areas where shortages already exceed EU averages [10,37]. Discussion of skills policy should therefore connect directly to assurance and auditability within the national ecosystem. The UK's Cyber Assessment Framework (CAF 4.0) illustrates how technical risk management can be mapped to demonstrable organisational capabilities and staff competence—an approach that could inform Lithuania's supervisory practices and sectoral guidance [57]. Concretely, embedding ECSF roles and proficiency levels into audit templates and tender requirements would convert abstract skills frameworks into enforceable market signals [46,51].

6.3. Quality Assurance and Signalling in Higher Education and CPD

The literature and stakeholder evidence converge on a persistent "theory–practice gap" in European cybersecurity education, with employers prioritising applied competence, certification, and experience over purely academic credentials [10,34]. The UK's dual track—NCSC-certified degrees and assured short courses—offers a pragmatic template. For Lithuania, a national cyber training quality label aligned with ECSF, and NIS2-related controls could (a) benchmark curricula against role profiles, (b) reward providers that integrate labs and internships, and (c) guide employer training budgets towards a validated provision (e.g., NCSC-driven programmes at the University of South Wales and UWE Bristol). Strategically, this label should be recognised in public procurement and supervisory guidance to ensure take-up and avoid a merely voluntary market of uneven quality [9].

In this context, Lithuania's HEIs face additional regulatory constraints to implement multidisciplinary cybersecurity programs and certification schemes posed by rigid national study-field descriptors, listing cybersecure only as a subject within the field of computing [4]. Although the descriptors were designed for broad disciplinary alignment, they now impede rapid curriculum adaptation to emergent labour market needs. Descriptors emphasise technical outcomes and require programmes to fit predetermined fields, limiting integration of soft, organisational, and managerial competencies alongside technical content. This tension hinders interdisciplinary programme development that blends human factors, risk governance, and communication skills, which employers increasingly value [10,58]. In this ambit, the development of stand-alone cybersecurity degrees—enabling focused depth—may struggle to cover non-technical domains. Cybersecurity specializations within broader IT or digital programmes, on the other hand, might offer curricular flexibility and resource efficiency but risk diluting core cybersecurity content, failing to produce fully job-ready graduates. Although clearer competency frameworks and more agile accreditation can help HEIs balance depth, breadth, and employer relevance in cybersecurity education,

the Lithuanian curricular landscape needs a deeper, participatory, multi-stakeholder review. Yet international trends in cybersecurity education reflect similar trends. Recent international studies suggest that although cybersecurity is increasingly used as a subject across technical disciplines, standalone study programs in full alignment with emerging standards for cybersecurity roles such as ENISA's ECSF framework, are still uncommon [58].

6.4. SMEs and the Practicality of Multi-Role Talent

SMEs dominate Lithuania's economy, and they cannot embed full ECSF roles. The policy question is therefore not whether every role is fulfilled, but how to bundle responsibilities safely and feasibly, balancing resource constraints, regulatory obligations, and operational priorities. Evidence shows that SMEs often seek "generalist-plus" practitioners—combining core IT with security, governance, and incident response—yet struggle to provide sustained upskilling [10,28]. The adoption and adaptation of the UK's approach to micro-credentials, short certified courses, and regional centres that deliver pooled lab facilities and training can help SMEs achieve baseline competence while reserving highly specialised services such as incident response and cyber-forensics to shared platforms (e.g., CyberFirst ecosystem and "Industry 100" initiatives). Lithuania's CyberHubs activities point in this direction but would benefit from broader institutionalisation, multi-year funding, and formal alignment to ECSF roles, and NIS2 controls to avoid project-bound discontinuity—the CyberHubs project ends in 2027 [4,10].

6.5. Early-Stage Pipeline and Inclusion as Capacity Multipliers

Sustained workforce growth requires early engagement, not solely mid-career reskilling. The UK's CyberFirst demonstrates how competitions, scholarships, and teacher support cultivate interest and diversify entry routes [49,52]. In this context, diversity is not simply an equity concern; it is a capacity lever in an undersupplied market, where women and minority groups remain under-represented but can decisively participate [2,34]. For Lithuania, national challenges, clubs, and scholarship schemes linked to visible career frameworks could mitigate demographic constraints and emigration pressures. Furthermore, embedding foundational cybersecurity content in secondary curricula—supported by universities and industry mentors—would gradually normalise cybersecurity as a mainstream pathway [9,10].

6.6. Skills Framework Architecture: ECSF as 'Lingua Franca'

The ECSF provides a common reference for roles, proficiency levels, and knowledge areas. Yet, adoption remains inconsistent, limiting its benefits for workforce planning and cross-border mobility [33,51]. In this ambit, Lithuania can lead implementation efforts by an early operationalising of the ECSF: not only by mapping national employment trends and patterns but by integrating ECSF levels into job descriptions and salary scales, in addition to requiring ECSF-referenced competence in public sector recruitment and procurement contracts. Although SMEs demand role consolidation, ECSF can still anchor competence coverage even if titles differ [46,49]. Over time, this could reduce the current mismatch between graduate outputs and employer needs by aligning curricula and assessments to role-specific learning outcomes [10,34].

6.7. From Policy to Practice: Governance Options for Lithuania

Considering the current governance framework, we argue that at least two institutional options emerge from the analysis. First, to consider establishing a National Cyber Skills Council embedded within existing cyber governance (e.g., under the MoD-NCSC umbrella), mandated to run rolling skills needs assessments, set competency benchmarks, and steward quality labels across HEIs, vocational, and training providers. Alternatively, this additional

role could be assigned directly to the NCSC, providing greater autonomy, coordination, and supervisory capabilities. Second, strengthening a networked model via a formalised CyberHubs-style consortium with statutory recognition and multi-year funding, acting as a skills integrator across ministries, universities, and industry [9,10,37]. In either case, policy leverage should flow through funding, procurement, and supervision: tie grants and recognition to ECSF-aligned outcomes, reward assured programmes, reflecting competence expectations in sectoral audit frameworks [47,57].

Summarising, Lithuania's next strategic phase should consider establishing long-term structures and mechanisms for the governance of its cyber needs, pairing standards with support by:

(1) Adopting ECSF as the organising vocabulary for roles and proficiency;
(2) Institutionalizing a national certified-training/degree label linked to NIS2-relevant competencies;
(3) Formalising governance to align ministries, HEIs, and industry;
(4) Funding modular, work-based learning schemes for SMEs, and shared regional capabilities; and
(5) Investing in school-to-work pathways with targeted inclusion measures.

Eventually, the transition from fragmented initiatives to a systemic, quality-assured, and auditable skills ecosystem is not only necessary and achievable but also integral to the regulatory compliance, resilience, and long-term digital competitiveness of the country [34,47,51].

6.8. Limitations and Future Work

This study relies on documentary analysis and expert-informed insights rather than primary labour-market microdata; consequently, some estimates and conclusions are subject to reporting biases and methodological variance across sources. Future research should triangulate employer-level data, graduate tracking, and audit outcomes to evaluate which interventions yield measurable improvements in competence and compliance readiness. Comparative evaluation of discussed initiatives, such as for example internship models, in other small EU economies would also clarify scalability and return on investments.

7. Conclusions

This study has examined the structural challenges facing cybersecurity skills development in Lithuania within the context of expanding European regulatory obligations, notably the NIS2 Directive. The findings demonstrate that Lithuania's skills gap extends beyond workforce shortages to encompass fragmented governance, limited quality assurance mechanisms, and weak alignment between education provision and labour-market demand. Drawing on a comparative analysis with the United Kingdom, the article has identified functionally transferable policy elements that may support a more coherent and sustainable national cybersecurity skills ecosystem.

Rather than advocating policy imitation, the analysis emphasises context-sensitive adaptation. Structured professional frameworks, recognised training and degree quality standards, institutionalised multi-stakeholder coordination, and integrated school-to-work pathways emerge as particularly relevant for a small, SME-dominated economy such as the Lithuanian one. The study further highlights the importance of operationalising European frameworks—especially the ECSF—not only as descriptive tools but as instruments embedded within recruitment practices, procurement, supervision, and curriculum design.

Ultimately, strengthening cybersecurity skills capacity is both a regulatory necessity and a strategic investment in national digital resilience. By moving from current fragmented, project-based initiatives towards an integrated, quality-assured, and auditable

skills system, Lithuania can enhance compliance readiness, support economic competitiveness, and build long-term resilience against evolving cyber threats. Future research should evaluate the effectiveness of these interventions through longitudinal workforce and employer-level data.

Author Contributions: Conceptualisation: C.C. and S.J.; validation and formal review: C.C., G.S. and S.J.; writing—original draft preparation: C.C. and S.J.; writing—review and editing: C.O., G.S. and O.H.; visualisation: C.C. and S.J.; supervision: G.S. and S.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was prepared as part of the project "Operationalizing Cyber Resilience in Critical Infrastructure: Protecting the Lithuanian Emergency Medical Services" (Project No. S-ITP-25-13), within the impact-driven programme "Information Technologies for the Development of Science and the Knowledge Society", funded by the state budget of the Republic of Lithuania administered via the Research Council of Lithuania ('Lietuvos Mokslo Taryba').

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study were derived from publicly available policy documents and academic literature as listed in the reference list. No new data were created or analysed in this study. Further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations were used in this manuscript:

ACE-CSR	Academic Centres of Excellence in Cyber Security Research
CAF	Cyber Assessment Framework
CISO	Chief Information Security Officer
CISP	Cyber security information sharing platform Connect Inform Share Protect
CYBERUK	Annual flagship UK government's cyber security event
CyBOK	Cyber Security Body of Knowledge
DAP	Digital Acceleration Programme
ECSF	European Cybersecurity Skills Framework
ENISA	European Union Agency for Cybersecurity
EPSRC	Engineering and Physical Sciences Research Council
EU	European Union
GDPR	General Data Protection Regulation
HEI	Higher Education Institution
ICT	Information and Communication Technologies
LTCYBERCOM	Lithuanian Cyber Command
MoD	Ministry of National Defence
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NIS2	Network and Information Security Directive 2
OSINT	Open-Source Intelligence
SME	Small and Medium-sized Enterprise
UK	United Kingdom
UWE	University of the West of England
UWTSD	University of Wales Trinity Saint David
VRI	Vulnerability Research Initiative

References

1. Odebade, A.T.; Benkhelifa, E. A comparative study of national cybersecurity strategies of ten nations. *arXiv* **2023**, arXiv:2303.13938.
2. ISC2. Global Cybersecurity Workforce. 2024. Available online: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study (accessed on 10 October 2025).
3. Blažič, B.J. The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technol. Soc.* **2021**, *67*, 101769. [CrossRef]
4. Bukauskas, L.; Brilingaitė, A.; Juozapavičius, A.; Lepaitė, D.; Ikamas, K.; Andrijauskaitė, R. Remapping cybersecurity competences in a small nation state. *Heliyon* **2023**, *9*, e12808. [CrossRef] [PubMed]
5. European Commission. Flash Eurobarometer 547. In *Cyberskills: Eurobarometer Report April–May 2023*; European Commission: Brussels, Belgium, 2024; ISBN 978-92-68-19470-6. [CrossRef]
6. Górka, M. Baltic States Cyber Security Policy: Development of digital capabilities in 2017–2022. *Stos. Międzynarodowe Int. Relat.* **2023**, *3*, 15. [CrossRef]
7. NIS Directive 2. Available online: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2 (accessed on 29 December 2025).
8. ENISA. Technical Implementation Guidance. Available online: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf (accessed on 29 December 2025).
9. OECD. *Building a Skilled Cyber Security Workforce in Europe: Insights from France, Germany and Poland (OECD Skills Studies)*; OECD Publishing: Paris, France, 2024. [CrossRef]
10. CyberHubs. Cybersecurity Skills Needs Analysis Report Lithuania. 2025. Available online: https://cyberhubs.eu/resource/cybersecurity-skills-needs-analysis-in-lithuania/ (accessed on 5 February 2026).
11. Bartlett, L.; Vavrus, F. Comparative case study research. In *Oxford Research Encyclopedia of Education*; Oxford University Press: Oxford, UK, 2019.
12. Shah, J.; Douglas, J.; Bollen, A.; Hasapopoulos, S.; Parmar, S.; Clarke, G.; Ipsos; Donaldson, S.; Perspective Economics. Cyber security Skills in the UK Labour Market and Cyber Security Sectoral Analysis 2025 Technical Report. Available online: https://assets.publishing.service.gov.uk/media/6893291f303b0dad411d4e50/Cyber_security_skills_in_the_UK_labour_market_2025_-_technical_report.pdf (accessed on 12 October 2025).
13. Cyber Security Skills in the UK Labour Market 2024: Technical Report, 2024. Available online: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024 (accessed on 3 November 2025).
14. The National Cyber Security Centre. Available online: https://www.ncsc.gov.uk/ (accessed on 29 December 2025).
15. Kallonas, C.; Stavrou, E. Expanding the cybersecurity workforce: Challenges, current practices and future directions in attracting and cultivating multidisciplinary talent. In *Proceedings of the IFIP World Conference on Information Security Education, Maribor, Slovenia, 21–23 May 2025*; Springer Nature: Cham, Switzerland; pp. 18–30.
16. National Cyber Strategy 2022. Pioneering a Cyber Future with the Whole of the UK. Available online: https://www.gov.uk/government/publications/national-cyber-strategy-2022 (accessed on 12 October 2025).
17. The Cyber Security Body of Knowledge. Available online: https://www.cybok.org/ (accessed on 29 December 2025).
18. CyberFirst. Available online: https://www.ncsc.gov.uk/cyberfirst/ (accessed on 29 December 2025).
19. Academic Centres of Excellence in Cyber Security Research. Available online: https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research (accessed on 10 October 2025).
20. NCSC Assured Training. Available online: https://www.ncsc.gov.uk/information/certified-training (accessed on 29 December 2025).
21. University of South Wales. Available online: https://www.southwales.ac.uk/cyber/ (accessed on 5 February 2026).
22. National Cyber Security Centre. Industry 100. Available online: https://www.ncsc.gov.uk/section/industry-100/about (accessed on 29 December 2025).
23. Cyber Essentials. Available online: https://www.ncsc.gov.uk/cyberessentials/overview (accessed on 29 December 2025).
24. NCSC. Research Institutes. Available online: https://www.ncsc.gov.uk/information/research-institutes (accessed on 29 December 2025).
25. Cyber Focus. Available online: https://www.lancaster.ac.uk/cybersecurity/cyber-focus/ (accessed on 28 December 2025).
26. UWE Bristol Is Providing "Gold Standard" Cybersecurity Education. Available online: https://www.uwe.ac.uk/news/uwe-bristol-providing-gold-standard-cyber-security-education?utm_ (accessed on 29 December 2025).
27. Apprenticeship in Computing (Computer Networks and Cybersecurity) (BSc Hons). Available online: https://www.uwtsd.ac.uk/programme-courses/undergraduate/computing/apprenticeship-computing-computer-networks-and (accessed on 27 December 2025).

28. Bada, M.; Nurse, J.R. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Inf. Comput. Secur.* **2019**, *27*, 393–410. [CrossRef]
29. CyberHubs. Available online: https://cyberhubs.eu/wp-content/uploads/2024/11/Summary-report_Cybersecurity-Skills-Needs-Analysis-1.pdf (accessed on 13 December 2025).
30. Almeida, F. Comparative analysis of EU-based cybersecurity skills frameworks. *Comput. Secur.* **2025**, *151*, 104329. [CrossRef]
31. Jacuch, A. Comparative analysis of cybersecurity strategies. European Union strategy and policies. Polish and selected countries strategies. *Online J. Model. New Eur.* **2021**, *37*, 102–120.
32. Spidalieri, F. Meeting the growing demand for cybersecurity skills and talent in Europe. In *European Cybersecurity in Context a Policy-Oriented Comparative Analysis, Proceedings of the European Liberal Forum, Brussels, Belgium, 24–25 September 2022*; European Liberal Forum (ELF): Brussels, Belgium; pp. 9–19. Available online: https://liberalforum.eu/wp-content/uploads/2022/08/European-Cybersecurity-in-Context_ELF-Study_Techno-Politics.pdf (accessed on 5 February 2026).
33. Spanou, D. The EU Cybersecurity Skills Academy: A silver bullet to address the cyber security skills gap in the European Union? *Cyber Secur. Peer-Rev. J.* **2024**, *7*, 229–236. [CrossRef]
34. ISACA. State of Cybersecurity 2025. Available online: https://www.isaca.org/resources/reports/state-of-cybersecurity-2025 (accessed on 28 December 2025).
35. Panko, M.; Šafár, L.; Mešťan, M. Small Firms, Big Threats: Cybersecurity Research and the Role of Public Policy in the SME Sector. *Cent. Eur. J. Public Policy* **2025**, *19*, 87. [CrossRef]
36. Štitilis, D.; Pakutinskas, P.; Laurinaitis, M.; de Castel, I.M.V. A Model for the National Cyber Security Strategy. The Lithuanian Case. *J. Secur. Sustain. Issues* **2017**, *6*, 357. [CrossRef] [PubMed]
37. Ministry of National Defence of the Republic of Lithuania. Lithuanian Cyber Defence Command. 2025. Available online: https://kam.lt/en/lithuanian-cyber-defence-command-opened/ (accessed on 29 December 2025).
38. Ministry of National Defence of the Republic of Lithuania. National Coordination Center. 2025. Available online: https://kam.lt/en/national-coordination-center/ (accessed on 29 December 2025).
39. Pedley, D.; Borges, T.; Bollen, A.; Shah, J.N.; Donaldson, S.; Furnell, S.; Crozier, D. *Cyber Security Skills in the UK Labour Market 2020*; Department for Digital, Culture, Media & Sport: London, UK, 2020.
40. Cram, W.A.; Yuan, J. Out with the old, in with the new: Examining national cybersecurity strategy changes over time. *J. Cyber Policy* **2023**, *8*, 26–47. [CrossRef]
41. NCC. Cybersecurity National Coordination Centre Lithuania (NCC). Ministry of National Defence. Available online: https://kam.lt/en/national-coordination-center/?utm_source=chatgpt.com (accessed on 15 January 2026).
42. EC. Lithuania: National Platform. Digital Skills and Jobs Platform. European Commission (EC). Available online: https://digital-skills-jobs.europa.eu/en/european-interactive-map/lithuania (accessed on 15 January 2026).
43. Trim, P.; Upton, D. *Cyber Security Culture: Counteracting Cyber Threats Through Organizational Learning and Training*; Routledge: London, UK, 2016.
44. Dawson, J.; Thomson, R. The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Front. Psychol.* **2018**, *9*, 744. [CrossRef] [PubMed]
45. Ullah, F.; Ye, X.; Fatima, U.; Akhtar, Z.; Wu, Y.; Ahmad, H. What Skills Do Cyber Security Professionals Need? *arXiv* **2025**, arXiv:2502.13658. [CrossRef]
46. Rathod, P.; Polemi, N.; Lehto, M.; Kioskli, K.; Wessels, J.; Lugo, R. Leveraging the European Cybersecurity Skills Framework (ECSF) in EU Innovation Projects: Workforce Development Through Skilling, Upskilling, and Reskilling. In *Proceedings of the IEEE Global Engineering Education Conference (EDUCON), Kos, Greece, 8–11 May 2024*; IEEE Computer Society: Los Alamitos, CA, USA, 2024. [CrossRef]
47. European Union. Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive). 2022. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (accessed on 9 December 2025).
48. ENISA. *NIS2 Directive: Cybersecurity Measures and Workforce Implications*; ENISA: Attiki, Greece, 2023. Available online: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (accessed on 10 December 2025).
49. UK Government. *National Cyber Strategy 2022*; HM Government: London, UK, 2022. Available online: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (accessed on 10 January 2026).
50. UK Cyber Security Council. Professional Standards and Career Pathways in UK Cybersecurity. 2023. Available online: https://www.ukcybersecuritycouncil.org.uk/for-individuals/become-professionally-registered/professional-standards (accessed on 9 January 2026).
51. ENISA. *European Cybersecurity Skills Framework (ECSF)*; European Union Agency for Cybersecurity: Attiki, Greece, 2022. Available online: https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf (accessed on 9 December 2025).
52. National Cyber Security Centre (NCSC). *NCSC Assured Training*; UK Government: London, UK, 2025. Available online: https://www.ncsc.gov.uk/information/certified-training (accessed on 5 February 2026).

53. Smith, G. The intelligent solution: Automation, the skills shortage and cyber-security. *Comput. Fraud Secur.* **2018**, *2018*, 6–9. [CrossRef]
54. Sundaramurthy, S.K.; Ravichandran, N.; Inaganti, A.C.; Muppalaneni, R. The future of enterprise automation: Integrating AI in cybersecurity, cloud operations, and workforce analytics. *Artif. Intell. Mach. Learn. Rev.* **2022**, *3*, 1–15.
55. Addula, S.R.; Tyagi, A.K.; Naithani, K.; Kumari, S. Blockchain-empowered Internet of things (IoTs) platforms for automation in various sectors. *Artif. Intell. Enabled Digit. Twin Smart Manuf.* **2024**, 443–477. [CrossRef]
56. Oladimeji, S.; Egon, A.; Broklyn, P. Cybersecurity Workforce Development: Bridging the Skills Gap in The Age of Automation. 2024. Available online: https://ssrn.com/abstract=4904939 (accessed on 5 February 2026).
57. NCSC. Cyber Assessment Framework 4.0. 2025. Available online: https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf (accessed on 29 December 2025).
58. Vykopal, J.; Švábenský, V.; Lopez, M.T.; Čeleda, P. Cybersecurity Study Programs: What's in a Name? In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1, Pittsburgh, PA, USA, 26 February–1 March 2025*; ACM: New York, NY, USA; pp. 1169–1175. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.