УДК 327

A GLOBAL SHORTFALL OF CYBER WORKFORCE: EVALUATING THE U.S. STRATEGY APPROACH AND UKRAINE'S EMERGING CHALLENGES

ГЛОБАЛЬНА КРИЗА З НЕСТАЧЕЮ КІБЕРФАХІВЦІВ: ОЦІНКА СТРАТЕГІЧНОГО ПІДХОДУ США ТА ВИКЛИКИ ДЛЯ УКРАЇНИ

Dmytro Dubov
Doctor of Political Sciences, Senior Research Fellow, Head of the Information Security and Cybersecurity Department of the Security Studies Center of the National Institute for Strategic Studies
e-mail: dubov@niss.gov.ua
ORCID ID: https://orcid.org/0000-0001-9728-369X

Svitlana Dubova
PhD in Historical Sciences, Head of the Board of the NGO “Center for Analysis and Development of Effective Policies”
e-mail: ngo.cadep@gmail.com
ORCID ID: https://orcid.org/0000-0002-0374-2099

Дмитро Дубов
Доктор політичних наук, старший науковий співробітник, завідувач відділу інформаційної безпеки та кібербезпеки центру безпекових досліджень Національного інституту стратегічних досліджень
e-mail: dubov@niss.gov.ua
ORCID ID: https://orcid.org/0000-0001-9728-369X

Світлана Дубова
Кандидат історичних наук, Голова правління Громадської організації «Центр аналізу та розробки ефективних політик»
e-mail: ngo.cadep@gmail.com
ORCID ID: https://orcid.org/0000-0002-0374-2099

***Abstract**. The article addresses the global shortage of cyber workforce, a challenge that directly impacts national security and international competition. The role of cybersecurity in large-scale military conflicts involving conventional weapons is examined, highlighting that while cyberspace has a limited direct impact on warfare, cybersecurity remains crucial for defense against cyberespionage and cyber sabotage. The study emphasizes that cybersecurity comprises three key components—technology, processes, and personnel—with the latter being the most critical. Effective technology use and process implementation depend on skilled professionals, their technological proficiency, and their awareness of cybersecurity’s significance in organizational operations. The article provides a detailed analysis of U.S. efforts to mitigate the cyber workforce shortage, including the National Cyber Workforce and Education Strategy, the first-year implementation report, and various legislative and local initiatives aimed at broadening workforce participation. Additionally, the strategies of specific agencies, such as the U.S. Department of Defense, for recruiting cybersecurity specialists are assessed.*

The study also explores Ukraine’s strategic approach to addressing the cybersecurity workforce deficit, noting the lack of attention to this issue in the country’s Cybersecurity Strategy and other national strategic documents. The current state of Ukraine’s cyber workforce is characterized by factors such as armed conflict, migration, and mobilization, the latter having helped address some staffing challenges in the security and defense sectors. A key barrier to effective policymaking in this area is identified as the absence of comprehensive statistical data. The article underscores the need to expand the cybersecurity talent pool by engaging traditionally underrepresented groups, including veterans, their spouses, women, and other social demographics.

***Keywords**: cyber workforce; cybersecurity; state policy; strategy; gaps; USA; Ukraine;*

***Анотація**. Стаття присвячена глобальній проблемі нестачі кібер робочої сили, що позначається на стані національної безпеки країн а відтак і міжнародному суперництві. Показна роль кібербезпекового фактору у масштабних військових конфліктах з використанням конвенційних озброєнь. Зокрема зазначено, що навіть незважаючи на обмежений вплив кіберпростору під час самого конфлікту, кібербезпека залишається важливим фактором адже сприяє захисту від кібершпигунства та кібердиверсій. Відмічено, що хоча кібербезпека складається з трьох компонентів: технології, процеси, люди, однак саме остання компонента є ключовою адже і ефективне використання технологій, і налагодження процесів критично залежить від навченого персоналу, його готовності до використання сучасних технологій, розуміння ролі кібербезпеки в функціонуванні організації. Докладно розглянуто ті заходи, яких вживало США для вирішення даної проблеми, в тому числі National Cyber Workforce and Education Strategy, звіт про її реалізацію за перший рік, а також ті локальні та законодавчі ініціативи яких вживали США аби розширити базу залучення кіберфахівців. Додатково розглянуто окремі відомчі стратегії залучення кіберфахівців (наприклад, Міністерства оборони США) та надано оцінку їх успішності. Проаналізовано стратегічні підходи до вирішення проблеми нестачі кіберфахівців в Україні. Зокрема вказано на брак уваги до цієї проблеми в Стратегії кібербезпеки України та інших стратегічних документах. Охарактеризовано поточний стан забезпечення України кіберробочою силою та фактори, які на це впливають: бойові дії, міграція та мобілізація (остання дозволила вирішити частину кадрових проблем організаціям сектору безпеки і оборони). Підкреслено, що базовою проблемою формування ефективної державної політики щодо проблеми є збір належних статистичних даних, які характеризують відповідну сферу. Зроблено акцент на необхідності розширення бази фахівців за рахунок ширшого залучення ветеранів, їх дружин, жінок та інших соціальних груп, які традиційно не охоплені цим процесом.*

***Ключові слова:** кіберфахівці; кібербезпека; державна політика; стратегія; прогалини; США; Україна;*

Introduction. Despite the increasing role of conventional military means in international relations in recent years, cybersecurity remains a critical element of modern conflicts. The ongoing Russian-Ukrainian war has reinforced the importance of maintaining strong armed forces while also revealing both the capabilities and limitations of cyberspace in military confrontations. Prior to the war, many cyber conflict theorists anticipated that cyber operations would play a role equal to, if not greater than, conventional warfare, with the potential for cyberattacks to dominate under favorable conditions. However, the reality of large-scale military-political conflicts suggests that the role of cyberspace is more limited, primarily encompassing cyber espionage and cyber sabotage, rather than directly shaping battlefield outcomes.

Cyber operations such as the attack on ViaSat in 2022, the attempted breach of Ukrtelecom, the 2023 cyberattack on Kyivstar, and the large-scale compromise of state registries in 2024, while significant in their media impact, did not have a decisive influence on the military conflict itself. Nevertheless, these incidents disrupted operations, diverted resources, and imposed reputational costs, forcing Ukraine to allocate additional funds for recovery efforts. Each attack aimed not only to cause operational disruptions but also to undermine public confidence in the state's ability to protect its citizens from cyber threats.

Given this landscape, cybersecurity remains a key pillar of national security. Neglecting it can lead to localized threats with potentially global repercussions. Effective cybersecurity relies on the synergy of three essential components: technology, processes, and people. While all three elements are crucial, the human factor is the cornerstone of this model. Trained professionals are essential for leveraging technology effectively, implementing secure processes, and understanding the strategic role of cybersecurity within an organization. This becomes even more apparent in offensive cyber operations, which require meticulous planning, network infiltration, and execution—areas where skilled personnel are indispensable.

The global shortage of cybersecurity professionals presents a significant challenge. By 2023, the shortfall had reached 3.4 million specialists (*Cybersecurity Workforce Demand, 2023*), rising to four million by April 2024 (*WEF Strategic Cybersecurity Talent Framework, 2024*). Experts from the World Economic Forum predict that this figure could escalate to 85 million by 2030 as digital dependency grows, exacerbated by emerging threats linked to artificial intelligence.

Some nations, such as the United States under President Biden, have recognized this workforce crisis and are implementing strategic policies to address the gap. Others, including Ukraine, are still in the early stages of developing solutions, facing unique challenges that further complicate efforts to build a robust cybersecurity workforce.

Literature review. While the challenges of cyber workforce training are widely covered in scientific literature, most studies focus on specific aspects or targeted measures aimed at improving particular segments of the issue. For instance, research by Manimay Dev and Debashis Saha (*Dev & Saha, 2023*), Amila Withanaarachchi and Nisansala Vithana (*Withanaarachchi & Vithana, 2022*), and Jing Zheng, Yuxin Pei, and Ya Gao (*Zheng, Pei, Gao, 2020*) examines the participation of women in cybersecurity and the obstacles they encounter. Other studies explore the learning process itself and strategies for optimizing it (*Lehto, 2016; Catota, Morgan, Sicker, 2019*; *Ashley, Kwon, Gourisetti, Katsis, Bonebrake, Boyd, 2022*) or focus on the necessary technical and cognitive skills for future cybersecurity professionals (*Dawson & Thomson, 2018*). However, the issue of developing a cohesive state policy on cybersecurity workforce remains insufficiently studied. This gap applies both to the analysis of individual national policies and to broader regional or international generalizations. Some studies attempt to address these broader issues, such as the work of Jared DeCrosta, who assesses the global state of the cybersecurity workforce, including models for measuring workforce shortages, and examines the impact of educational systems and public policies on the availability of skilled professionals (*DeCrosta, 2021*). Another key study in this area is by Chooi Shi Teoh and Ahmad Kamil Mahmood (*Teoh & Mahmood, 2017*), who analyzed nine National Cybersecurity Strategies from developed countries to determine whether they address cybersecurity workforce development. Their main conclusion is that while most countries acknowledge the importance of cyber workforce growth in their strategies, these references are often too general and lack concrete policy measures. A significant study directly related to the formulation of state policy is the analytical essay by William Crumpler and James A. Lewis (*Crumpler & Lewis, 2019*), which examines the overall U.S. approach to cybersecurity workforce development. The authors emphasize the need for stronger government support for retraining programs, professional competitions, soft skills development, and the expansion of the National Network of Academic Centers of Excellence as a foundation for public policy in this field.

The purpose of the article to conduct a comprehensive analysis of U.S. state policy on addressing cybersecurity workforce challenges and to outline initial perspectives on the issues facing Ukrainian state policy in this area.

Main results of the research. US policy on overcoming the cyber workforce gap. As of June 2024, official data indicates that there were 500,000 unfilled cybersecurity positions in the United States. This workforce shortage poses a significant strategic threat to U.S. national security, a concern highlighted by FBI Director Christopher Wray in 2023: "Even if all FBI cyber agents and intelligence analysts focused solely on threats from China, Chinese hackers would still outnumber them at least 50 to one" (*Media Advisory, 2023*).

A study conducted by CyberSeek in collaboration with the U.S. National Institute of Standards and Technology (NIST), a key organization responsible for setting cybersecurity standards and educational requirements, estimates that the total number of cybersecurity professionals in the U.S. is approximately 1.2 million (*CyberSeek, 2024*). However, this remains critically insufficient given the rapid evolution of digital technologies and the country's growing dependence on digital solutions. One contributing factor to this shortage is the perception of cybersecurity as a male-dominated field, with women comprising only about 24% of the cyber workforce (*Cybersecurity Workforce Report, 2024*).

The issue of cybersecurity workforce shortages was formally recognized in the National Cybersecurity Strategy released in March 2023 (*The National Cybersecurity Strategy, 2023*). The document acknowledges that both government agencies and the private sector struggle to recruit and retain cybersecurity professionals, posing a direct risk to national security. Given the complexity of the problem, a dedicated strategy was deemed necessary, leading to the development of the National Cyber Workforce and Education Strategy (*National Cyber Workforce and Education Strategy, 2023*), which was assigned to the Office of the National Cyber Director (ONCD).

In July 2023, the Office of the National Cyber Director (ONCD) released the National Cyber Workforce and Education Strategy. The strategy is built around four key pillars that guide all related initiatives:

- Ensuring that all Americans possess fundamental cybersecurity skills
- Transforming cybersecurity education
- Expanding and strengthening the overall U.S. cyber workforce
- Enhancing the capabilities of existing federal cybersecurity professionals

The strategy emphasizes that the scale of the issue requires a deliberate state policy aimed at maximizing the pool of future cybersecurity professionals. It stresses the need to include individuals from all backgrounds, regardless of age or demographic group, specifically mentioning women, veterans, military spouses, people of color, first-generation professionals, individuals with disabilities, members of LGBTQ+ communities, Indigenous groups, and residents of areas with limited access to educational opportunities.

The four main goals outlined in the strategy led to the definition of 15 strategic objectives that guide its implementation. These objectives include:

- Developing national initiatives to raise public awareness of cybersecurity skills
- Establishing a presidential award for achievements in basic cybersecurity skills
- Promoting the development of international standards related to cybersecurity skills
- Supporting and strengthening regional cybersecurity education systems
- Engaging the private sector and local communities in the development and support of training programs
- Integrating practical cybersecurity content into interdisciplinary educational programs
- Expanding access to cybersecurity education curricula
- Improving data accessibility on the cybersecurity workforce
- Increasing access to free or low-cost workforce development tools for small businesses and nonprofit organizations
- Leveraging professional learning communities to enhance workforce diversity and better align with labor market needs
- Encouraging skills-based hiring practices in both the public and private sectors
- Expanding experiential learning opportunities, such as internships and work-readiness programs
- Promoting flexible employment models, including part-time work
- Increasing the participation of veterans and their families in the cybersecurity workforce
- Streamlining hiring processes within federal agencies
- Expanding employment opportunities for graduates and young professionals in federal agencies
- Providing access to retraining and professional development programs for cybersecurity professionals

The head of ONCD is personally involved in promoting the goals of the strategy. In June 2024, the first report on its implementation was published (*Initial Stages of Implementation, 2024*). The document does not assess how much the situation in this area has changed but instead lists measures taken by federal and non-governmental entities to achieve the strategy's objectives.

One of the key initiatives is the transition to qualification-based hiring, which places less emphasis on formal educational requirements and more on actual cybersecurity qualifications, such as certifications or practical assessments. The government has also launched Tech to Gov job fairs to attract cyber professionals, with the second fair held in April 2024, attracting 1,700 participants.

A program has been introduced to designate educational institutions as National Centers of Academic Excellence in Cybersecurity (NCAE-C). This status reflects a high level of professional training recognized by the government, provides access to additional federal funding, and ensures that training programs align with the NICE Framework developed by NIST, which defines the relationship between skills and specific cybersecurity roles.

National Coordinator for Critical Infrastructure Security and Resilience or CISA (*CISA's Vulnerability Management, 2024*) has joined the Neurodiverse Federal Workforce program to recruit individuals with autism spectrum disorders for cybersecurity positions. Other initiatives mentioned in the report include the Cyber Clinics model, which engages university students in solving cybersecurity challenges for small businesses and local communities, a national roadshow by ONCD to major educational institutions to highlight the importance of cybersecurity professionals in federal agencies, and increased attention to the US President's Cybersecurity Cup, where teams from more than 100 agencies compete in cyber threat scenarios, with the winner recognized at a White House event.

In addition to the national strategy, some federal agencies have developed their own departmental strategies to attract cybersecurity professionals. In March 2023, the US Department of Defense adopted its own strategy (*DOD Cyber Workforce Strategy 2023-2027, 2023*). While the document does not provide estimates of the overall workforce gap, sources indicate that at the time of its adoption, approximately 25% of cybersecurity positions within the Department of Defense were unfilled. By November 2024, a year after its implementation, this figure had dropped to 16%, though 28,000 vacancies remained (*Pomerleau, 2024*). One significant factor contributing to this improvement may be the transition to qualification-based hiring rather than relying on minimum education requirements (*Eric Hysen, 2024*), which has expanded opportunities for individuals who previously would not have been eligible for such positions.

American lawmakers are also seeking solutions to this workforce shortage. In November 2023, Senator Margaret Wood Hassan introduced the Federal Cybersecurity Workforce Expansion Act (*Federal Cybersecurity Workforce Expansion Act, 2023*). If passed, the bill would establish two five-year programs. The first would create an apprenticeship program for 25 participants annually, funded through grants from the Department of Homeland Security (DHS), requiring participants to commit to working in federal cybersecurity roles for a specified period. The second program would provide cybersecurity training for veterans and military spouses, particularly those without higher education, focusing on practical skills and offering graduates opportunities to work in federal agencies.

In May 2024, Congresswoman Shontel M. Brown introduced the Diverse Cybersecurity Workforce Act of 2024 (*Diverse Cybersecurity Workforce Act, 2024*). This bill proposes a nationwide information campaign led by CISA to encourage individuals from underrepresented communities, including those with prior incarceration, to enter the cybersecurity field.

It remains unclear how the change in the US government in 2025 will impact these trends. While the new Trump administration has expressed opposition to DEI initiatives, which were considered in the previously mentioned policies, their cancellation will not resolve the cybersecurity workforce shortage. Additionally, tighter immigration restrictions could further exacerbate the issue, as the United States has previously implemented specific immigration programs for cybersecurity professionals, such as the H-1B visa. Even if the Trump administration limits these pathways for recruiting cyber talent, the growing cybersecurity challenges and workforce demands will persist, requiring alternative solutions.

Ukraine faces new and old challenges of cyber workforce gap. Like in the United States, the shortage of cybersecurity specialists is a pressing issue in Ukraine. Both the public and private sectors are expanding rapidly, creating an increasing demand for skilled professionals. According to the Aspen Institute (*Overview of the cybersecurity market in Ukraine, 2025*), the Ukrainian cybersecurity market was valued at 138 million USD in 2024. While this figure is modest compared to other countries—800 million USD in Poland and 8 billion USD in Germany—it represents a fourfold increase since 2016.

The main challenges in recruiting cybersecurity professionals in Ukraine's public and private sectors have traditionally included a shortage of qualified specialists, low salaries in the public sector, a lack of understanding among leadership regarding the value of cybersecurity professionals, and the high demand for experienced Ukrainian cyber experts from foreign companies.

The full-scale war has partially altered this landscape. Security and defense authorities responsible for cybersecurity, as outlined in the Law on the Basic Principles of Cybersecurity in Ukraine (*On the basic principles of cybersecurity in Ukraine Law, 2017*), have addressed staffing shortages through mobilization. However, some cyber specialists have left the country for various reasons, while others have been assigned to non-cyber units within the Armed Forces of Ukraine, limiting their ability to contribute their expertise. Meanwhile, cyber threats to critical infrastructure, including both government and private sector organizations, remain a significant concern.

Even if the broader military-political situation does not change, Ukraine could face a long-term cybersecurity workforce crisis in the near future. The current National Cybersecurity Strategy of Ukraine (*National Cybersecurity Strategy of Ukraine, 2021*) does not adequately address this issue. While some provisions emphasize professional development for security and defense personnel (paragraphs 25, 26, 62), financial incentives (paragraph 61), and private sector involvement in countering cyber threats (paragraphs 34 and 35), only paragraph 58 explicitly mentions improving cybersecurity training. However, the Strategy (and even Implementation Plan) does not yet provide clear directions for its implementation.

Although cybersecurity workforce challenges may seem secondary in the context of conventional warfare, they could become a crucial tool for social adaptation in the long term, particularly if the military-political situation changes significantly.

One of Ukraine's primary issues in this area is the lack of a systematic assessment of its cybersecurity workforce. The state does not have precise data on the number of vacant cybersecurity positions in either the public or private sectors, has limited insight into the challenges of specialist training, and lacks detailed information on workforce demographics, such as gender, ethnicity, and age distribution. While there is a slightly better understanding of the potential talent pool, the commonly stated shortage of cybersecurity specialists is more of a general consensus among professionals than a statistically verified fact.

At the same time, given ongoing migration trends and the current social structure, Ukraine should already be exploring ways to attract new target groups to the cybersecurity sector through expanded training programs. These groups include veterans, their spouses, women, and other vulnerable populations. This is particularly relevant for veterans, who represent a large social group in need of long-term reintegration, often requiring training in new professions. While some international projects, in collaboration with government agencies, offer ad hoc retraining programs, their effectiveness and long-term impact remain difficult to assess.

A similar challenge exists in increasing women's participation in cybersecurity. Although initiatives like the National Security and Defense Council's National Initiative to Strengthen the Role of Women in Cybersecurity play an important role, a more comprehensive policy is needed to define clear objectives and implementation steps.

Conclusions. A global shortage of 3.4 million cybersecurity professionals poses a serious risk to the security of even the most developed countries. Various hostile actors, both financially motivated and state-sponsored, are actively exploiting this workforce gap to their advantage. As a result, governments are increasingly focusing not only on improving cybersecurity training but also on attracting new professionals to the field.

In the United States, the cybersecurity workforce shortage stands at approximately 500,000 across both public and private sectors. To address this issue, the Biden administration adopted the National Cyber Workforce and Education Strategy in 2023, assigning its implementation to the

National Cyber Director, one of the highest-ranking officials in U.S. cybersecurity. These national efforts were further reinforced by local initiatives, agency-level strategies, and legislative proposals aimed at expanding the cybersecurity workforce. Although the first annual report on the strategy's implementation highlighted significant efforts to address the problem, it did not provide a quantitative assessment of progress. The change in U.S. leadership in 2025 may introduce additional challenges, particularly due to shifts in migration and domestic policies, which could force alternative solutions or leave federal information systems and critical infrastructure more vulnerable to cyber threats from Russia and China.

For Ukraine, the cybersecurity workforce shortage is further compounded by several additional factors, including the absence of a dedicated national strategy, limited resources, ongoing military conflict, workforce displacement, and demographic shifts. Addressing this issue requires at least a foundational policy to attract cybersecurity professionals and expand recruitment efforts among underrepresented social groups, such as women, veterans, and military spouses. Beyond addressing workforce needs, such initiatives would also contribute to the professional development and social reintegration of these groups.

References.

1. Cybersecurity Workforce Demand (2023), NIST, https://www.nist.gov/system/files/documents/2023/06/05/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf
2. WEF Strategic Cybersecurity Talent Framework (2024), World Economic Forum, https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf
3. Dev, M. and Saha, D. (2024), "Does e-government development moderate the impact of female labor participation on national cybersecurity maturity? An empirical investigation", *Information and Computer Security*, Vol. 32 No. 1, pp. 74-92. https://doi.org/10.1108/ICS-03-2023-0042
4. Withanaarachchi, A. and Vithana, N. (2022), "Female underrepresentation in the cybersecurity workforce – a study on cybersecurity professionals in Sri Lanka", Information and Computer Security, Vol. 30 No. 3, pp. 402-421. https://doi.org/10.1108/ICS-08-2021-0129
5. Zheng, J., Pei, Y., Gao Y. (2020) Social Media as a Disguise and an Aid: Disabled Women in the Cyber Workforce in China, Vol 8, No 2 (2020): Left Behind? Women's Status in Contemporary China, https://doi.org/10.17645/si.v8i2.2646
6. Lehto, Martti. 2016. Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences. Int. J. Cyber Warf. Terror. 6, 2 (April 2016), 15–31. https://doi.org/10.4018/IJCWT.2016040102
7. Frankie E Catota, M Granger Morgan, Douglas C Sicker, Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz001, https://doi.org/10.1093/cybsec/tyz001
8. T. D. Ashley, R. Kwon, S. N. G. Gourisetti, C. Katsis, C. A. Bonebrake and P. A. Boyd, (2022) "Gamification of Cybersecurity for Workforce Development in Critical Infrastructure," in IEEE Access, vol. 10, pp. 112487-112501, , doi: 10.1109/ACCESS.2022.3216711
9. Dawson J and Thomson R (2018) The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Front. Psychol. 9:744. doi: 10.3389/fpsyg.2018.00744
10. DeCrosta, Jared (2021). Bridging the Gap: An Exploration of the Quantitative and Qualitative Factors Influencing the Cybersecurity Workforce Shortage // Utica College ProQuest Dissertations & Theses, 2021, https://www.proquest.com/openview/b08d412275c53f095c3f145e30717ab6/1?pq-origsite=gscholar&cbl=18750&diss=y
11. Teoh, C. S., & Mahmood, A. K. (2017). Cybersecurity Workforce Development for Digital Economy. The Educational Reviewing, USA,2(1), 136-146.

http://dx.doi.org/10.26855/er.2018.01.003 , https://www.researchgate.net/profile/Efthymia-Gourgiotou/publication/323834705_Trainee_Teachers'_Collaborative_and_Reflective_Practicum_in_Kindergarten_Classrooms_in_Greece_A_Case_Study_Approach/links/5aae2611aca2721710fb0e7f/Trainee-Teachers-Collaborative-and-Reflective-Practicum-in-Kindergarten-Classrooms-in-Greece-A-Case-Study-Approach.pdf#page=23

12. Media Advisory (2023) Chairman Green Announces Hearing on America's Cyber Workforce Shortage Amid Rising Threats, Homeland Security Committee, https://homeland.house.gov/2024/06/21/media-advisory-chairman-green-announces-hearing-on-americas-cyber-workforce-shortage-amid-rising-threats/

13. CyberSeek (2024) 225,000 More Cybersecurity Workers Needed in US, https://www.securityweek.com/225000-more-cybersecurity-workers-needed-in-us-cyberseek/

14. Cybersecurity Workforce Report (2024) Bridging the Workforce Shortage and Skills Gap, Global Cybersecurity Forum, https://web-assets.bcg.com/61/d3/705fbd684d70b0e5f98cdcf7cf47/2024-cybersecurity-workforce-report.pdf

15. The National Cybersecurity Strategy (2023), White House, https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/

16. National Cyber Workforce and Education Strategy (2023), Scribd.com, https://www.scribd.com/document/680371021/NATIONAL-CYBER-WORKFORCE-AND-EDUCATION-STRATEGY

17. Initial Stages of Implementation (2024) National Cyber Workforce and Education Strategy, Biden White House.Archives, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf

18. CISA's Vulnerability Management (2024), CISA, https://www.cisa.gov/news-events/news/cisas-vulnerability-management-goes-big-interns-and-results-are-staggering

19. DOD Cyber Workforce Strategy 2023-2027 (2023), Department of Defense, https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf

20. Pomerleau, Mark (2024) DOD sees decrease in civilian cyber workforce shortage amid efforts to beef up talent pipeline, DefenseScoop, https://defensescoop.com/2024/11/07/dod-sees-decrease-civilian-cyber-workforce-shortage-talent-pipeline/

21. Eric Hysen (2024) Testimony of Eric Hysen Chief Information Officer and Chief Artificial Intelligence Officer

22. U.S. Department of Homeland Security before Committee on Homeland Security United States House of Representatives on "Finding 500,000: Addressing America's Cyber Workforce Gap", Committee on Homeland Security, https://homeland.house.gov/wp-content/uploads/2024/06/2024-06-26-HRG-Testimony.pdf

23. Federal Cybersecurity Workforce Expansion Act (2023), US Congress, https://www.congress.gov/bill/118th-congress/senate-bill/2256

24. Diverse Cybersecurity Workforce Act (2024), US Congress, https://www.congress.gov/bill/118th-congress/house-bill/8469/all-actions?q=%7B%22search%22%3A%22Diverse+Cybersecurity+Workforce+Act+of+2024%22%7D&s=1&r=1&overview=closed#tabs

25. Overview of the cybersecurity market in Ukraine (2025), Aspen Institute, https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf

26. On the basic principles of cybersecurity in Ukraine Law (2017), Verhovna Rada of Ukraine, https://zakon.rada.gov.ua/laws/show/2163-19#Text

27. National Cybersecurity Strategy of Ukraine (2021), President of Ukraine site, https://www.president.gov.ua/documents/4472021-40013