ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

Proposed Standards for Cybersecurity Curricula in Higher Education

Stavros E. Basta[1]; Dr. Ihssan Alkadi[2]; Rebecca M. Basta[3]

[1,3]R & S Educational Consultants Inc.

[2]Full Professor of Computer Science & Cybersecurity, North Greenville University

Publication Date: 2026/03/20

Abstract:

- ***Background/Purpose:***

Cybersecurity has become a critical concern across national security, industry, and academia, yet higher education institutions lack a unified, standardized curriculum framework for training cybersecurity professionals. Unlike established disciplines such as medicine or accounting, cybersecurity programs vary widely in content, depth, and pedagogical approach, resulting in inconsistent graduate competencies, persistent workforce shortages, and a growing misalignment between academic preparation and industry demands. This paper addresses the urgent need for proposed standards that can guide the development of coherent and comprehensive cybersecurity curricula at both the undergraduate and graduate levels.

- ***Methods:***

This study employs a comprehensive review and synthesis of major accreditation frameworks and curriculum guidelines, including ABET computing accreditation criteria, NSA/DHS Centers of Academic Excellence (CAE) designation requirements, the NIST/NICE Cybersecurity Workforce Framework, ACM/IEEE Cybersecurity Curricula Guidelines (CSEC2017), and industry certification pathways (e.g., CompTIA Security+, CISSP, CEH). By analyzing and cross-referencing these frameworks, the study proposes integrated year-by-year curriculum models for both undergraduate and graduate programs, mapping core knowledge areas, hands-on competencies, and professional development milestones.

- ***Results/Findings:***

The analysis reveals significant gaps and inconsistencies across existing cybersecurity programs, including inadequate hands-on training, outdated course content, weak alignment between academic curricula and industry certifications, and disparities in institutional resources and faculty expertise. The paper presents structured four-year undergraduate and graduate curriculum standards encompassing foundational computing, core cybersecurity knowledge areas (network security, cryptography, secure software development), applied specializations (digital forensics, penetration testing, cloud security), and capstone experiences. It further identifies key barriers to standardization, such as balancing academic freedom with national standards and addressing resource inequities among institutions.

- ***Conclusions:***

Establishing standardized, competency-based cybersecurity curricula aligned with recognized frameworks is essential to closing the cybersecurity skills gap and producing workforce-ready graduates. The paper recommends universal adoption of the NIST NICE framework, sustained collaboration among academia, industry, and government, dedicated investment in faculty development and laboratory infrastructure, and formalized processes for continuous curriculum review. These standards provide a scalable foundation for institutions to build rigorous, adaptive, and industry-relevant cybersecurity programs.

Keywords: *ABET Accreditation, Centers of Academic Excellence (CAE), Curriculum Standardization, Cybersecurity Education, Cybersecurity Workforce, Higher Education, Industry Certifications, NIST NICE Framework, Undergraduate and Graduate Programs.*

How to Cite: Stavros E. Basta; Dr. Ihssan Alkadi; Rebecca M. Basta (2026) Proposed Standards for Cybersecurity Curricula in Higher Education. *International Journal of Innovative Science and Research Technology*, 11(3), 1481-1492. https://doi.org/10.38124/ijisrt/26mar896

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

I. INTRODUCTION

➢ *Overview*

The rising need for strong cybersecurity across national security, industry, and universities highlights an urgent requirement: creating educational programs that develop skilled people who can handle tough cybersecurity issues. Cyberattacks are happening more often, showing weaknesses in important infrastructure, and it's becoming clear that current education isn't good enough. The lack of consistent cybersecurity education leads to big differences in the skills and abilities of graduates. This results in job openings that can't be filled, making the problems even worse (Tikanm Iäki et al., 2025)(Jerman-Blazic A et al., 2024). Because of this, we need to take action and create standardized curricula. These programs should give students the knowledge they need and match what the cybersecurity world requires as it changes (Stavrou E et al., 2024). Having clear guidelines for both undergraduate and graduate programs is essential, ensuring that the curricula are complete and can adapt to new technologies and threats quickly. It's important to acknowledge accreditation's role in maintaining quality in cybersecurity education. Groups like ABET (Accreditation Board for Engineering and Technology) offer frameworks that confirm programs meet high standards and prepare students well for their careers (Tay A et al., 2024). Also, designations from the NSA (National Security Agency) for Centers of Academic Excellence (CAE) add credibility and structure, helping schools create curricula that meet national security and job market needs (Dubinsky V, 2024)(Avrahami Z et al., 2025). These accreditations stress the need to follow standards and curriculum guidelines, like those from NIST (National Institute of Standards and Technology) and NICE (National Initiative for Cybersecurity Education) (Yang Y et al., 2025). These help align what students learn with the skills they need for their jobs. To properly train future cybersecurity experts, a standard curriculum needs to cover many key areas. For undergraduates, a basic understanding of information security, network protocols, and software security is essential. They should also know the ethical, legal, and policy rules of cybersecurity, allowing them to work within complex regulations (Ramezanian S et al., 2024)(Segate RV, 2024). Moreover, curricula should include strong training in both defensive and offensive strategies, with practical lab work to improve problem-solving and critical thinking (J R K Bokau et al., 2024). This approach strengthens their understanding of theory and builds the technical skills needed for real-world cybersecurity challenges. In graduate programs, education should shift to more advanced topics like cryptography, secure systems, and cyber operations.

➢ *Introduction: High Demand of Cybersecurity in National Security, Industry, and Academia.*

The interwoven nature of national security, industry needs, and academic efforts regarding strong cybersecurity shines a light on the critical need for well-rounded education in this arena. Cyber threats are becoming more sophisticated and common, and their effects are now felt far beyond single businesses, impacting entire economies and critical national infrastructure. Federal bodies like the Department of Homeland Security (DHS) and CISA have stressed how vital it is to grow a skilled group ready to handle these varied issues. These threats include everything from data breaches in companies to potential cyberattacks on key national assets, necessitating a response involving not only tech skills but also policy creation and rollout (Tikanm Iäki et al., 2025). The private sector is seeing a huge rise in the need for cybersecurity experts; research indicates a large gap between available roles and qualified individuals (Jerman-Blazic A et al., 2024). This shortage hurts businesses' ability to deal with threats and is also a major block to national security goals, calling for a quick, strategic focus on cybersecurity education (Stavrou E et al., 2024). In academic circles, matching what's taught to the demands of industry and national security is super important. Educational institutions realize that a lack of consistent educational approaches contributes to the skills deficit; many programs just don't cover key skills needed in today's cybersecurity world (Tay A et al., 2024). Groups like NICE and the NSA have taken steps to fix this by suggesting curriculum standards that outline essential skills for cybersecurity folks (Dubinsky V, 2024). Still, it's not just about designing courses that meet these benchmarks; it's also about making sure they're taught well across different schools. Different schools have different resources and ways of teaching, making it hard to create a standard way of doing things (Avrahami Z et al., 2025). Therefore, program accreditation is vital in proving the worth of cybersecurity education programs. Accreditation makes sure academic programs are good and thorough, while also making communication between schools and the cybersecurity field smoother.

The demand for needed and improved cybersecurity awareness and improved security methods and techniques has risen in recent years because cyber threats are more advanced, widespread, and damaging. Below are real-world examples and categories that illustrate why cybersecurity awareness and investment are in such high demand today:

1. Ransomware Attacks on Critical Infrastructure: Colonial Pipeline (2021), 2. Healthcare Breaches and Data Theft: Anthem Healthcare Breach (2015) and Change Healthcare (2024), 3. Education Sector Targeted: Los Angeles Unified School District (LAUSD) Ransomware Attack (2022), 4. Corporate Espionage and Phishing: Twitter Employee Social Engineering (2020), 5. Massive Retail Data Breaches: Target Breach (2013), 6. Remote Work and Cloud Security Risks: Zoom and Remote Work Exploits (2020–present), 7. Government and Election Security: U.S. Federal Agency Breach via SolarWinds (2020), 8. Rise of Personal Cybercrime: Identity Theft and Financial Scams. 90% of breaches are caused by weak human security practices or phishing. Cyber threats are more sophisticated and more advanced and faster than policies, that is why continuous awareness helps people adapt. Technology alone isn’t sufficient; users must be constantly trained as it becomes a much-needed defense mechanism.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

- *Research Motives: Lack of Standardization in Cybersecurity Education can Cause Vacancies in Skill and Performance*.

Cybersecurity as a field does not have a standardized and accepted curriculum framework. Not such as accounting (with CPA standards) or medicine (with board certifications). Schools, certification centers, and training centers define "cybersecurity" in different ways. This causes inconsistent graduate skillsets and confusion among employers.

Another issue is certification vs. academic misalignment. Where Industry certifications (e.g., CompTIA Security+, CISSP, CEH, AWS Security) focus on practical, up-to-date skills. University curricula often lack updating. Graduates may lack hands-on readiness for modern attacks, while certified professionals lack theoretical grounding. There are some Missing or Weak courses in cybersecurity curricula due to omitted importance or outdated material. Consequences of This lack of standardization causes employers to face hiring confusion and job candidates have inconsistent skill sets.

- *Goals: To Set Standards that Guide the Development of Cybersecurity Curricula for Undergraduate and Graduate Programs.*

Cybersecurity is as crucial as traditional engineering or healthcare, and academic programs vary significantly in how and what they teach. There must be universally core competencies across academic institutions, and proper coordination between academic theory and workforce skillsets needed, and speedy adaptations to sophisticated and improving cyber threats. Standards must be competency-based curriculum framework. Every program should align with a recognized competency model that defines: Core knowledge areas (e.g., networks, cryptography). Hands-on knowledge (e.g., secure coding, incident response). Students must graduate with various operational experience, not just theoretical education. There must be alignment with Industry Certifications Entry-level: CompTIA Security+, Network+, Cisco CCNA Security, Mid-level: CEH, CISSP, GIAC GSEC, and Cloud: AWS/Azure Security Specialty. Annual continuous curriculum review & updating since Cybersecurity changes rapidly. Use and apply Frameworks to implement These Standards. Frameworks include NIST NICE Framework (U.S.), NSA / DHS CAE-CD, ABET Computing Accreditation, ACM/IEEE Cybersecurity Curricula Guidelines (CSEC2017), ISO/IEC 27001 & 27032

II. ROLE OF ACCREDITATION IN ASSURING PROGRAM STANDARD OF STUDENT'S PERFORMANCE IN CYBERSECURITY

Accreditation is important for making sure cybersecurity programs, both for undergrads and graduates, meet the standards everyone agrees on. This helps students do better and get ready for jobs. Groups like ABET and the NSA, with its CAE program, have come up with rules schools have to follow to get accredited. These rules don't just check if the school is good; they also make sure what students learn matches what the country needs for security and what companies are looking for. So, it kind of closes the gap between what's taught and what skills you need in cybersecurity (Tikanm Iäki et al., 2025)(Jerman-Blazic A et al., 2024). Getting accredited means a thorough check to see if the programs are meeting their goals and if students are learning what they should do well in cybersecurity jobs. Using specific guidelines and standards, like the ones from NIST and NICE, makes the programs more consistent and relevant (Stavrou E et al., 2024)(Tay A et al., 2024). These standards highlight key knowledge areas such as managing information security, figuring out risks, and the legal stuff and ethics around cybersecurity. Besides the national standards, the ISO/IEC 27000 standards give a good structure for managing information security. This helps schools match their courses with the best practices from around the world, which gets students ready for working in a global industry (Dubinsky V, 2024). Also, the ACM/IEEE curriculum guidelines are a base for making detailed programs in computers and cybersecurity, which really helps in deciding how the program should be set up and what to teach.

- *ABET Accreditation for Computing and Cybersecurity Programs.*

Accreditation holds a crucial position in both establishing and upholding rigorous educational standards in cybersecurity and computing programs. This, in turn, directly influences the quality of graduates and their readiness for the ever-changing challenges within this domain. The Accreditation Board for Engineering and Technology, or ABET, offers a widely respected framework. This framework assesses programs against tough criteria. It ensures programs effectively educate on both theoretical and hands-on cybersecurity aspects. This accreditation tells stakeholders (like potential students, employers, and the broader industry) that the program maintains certain quality assurance metrics. These metrics should meet professional expectations in computing (Tikanm Iäki et al., 2025). ABET accreditation places importance on continuous improvement. It pushes institutions to always evaluate and improve their curricula as technology and the market evolve (Jerman-Blazic A et al., 2024). This ongoing process raises educational quality. It also boosts program credibility. This, in turn, helps meet the nation's need for highly skilled cybersecurity pros (Stavrou E et al., 2024).NSA and DHS Centers of Academic Excellence (CAE) designations also show an institution's dedication to high-quality cybersecurity education. Meeting stringent requirements related to curriculum, faculty, and community involvement is necessary for these designations (Tay A et al., 2024). Designated institutions gain visibility and may see increased funding for cybersecurity R&D (Dubinsky V, 2024). The combination of ABET accreditation and CAE designations creates a robust system of educational standards. This system aims to cultivate a skilled cybersecurity workforce capable of understanding and combating the increasing cyber threats we face (Avrahami Z et al., 2025).

ABET recommended Cybersecurity Course plan include:

- *Year 1 – Foundations of Computing and Security*

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

✓ *Fall*

- Introduction to Cybersecurity Cross-cutting concepts (CIA triad, risk)

✓ *Spring*

- Programming II / Data Structures
- Computer Hardware & Operating Systems
- Networking Fundamentals
- Ethics in Technology Ethics

- *Year 2 – Core Cybersecurity Knowledge*

✓ *Fall*

- Computer & Network Security
- System security
- Database Systems & Security Data security
- Secure Software Development

✓ *Spring*

- Cryptography & Data Protection
- Human Factors in Cybersecurity
- Security Policies & Risk Management Organizational security
- Scripting for Cybersecurity (Python, Bash)

- *Year 3 – Applied and Specialized Topics*

✓ *Fall*

- Incident Response & Digital Forensics
- Web & Application Security
- Cloud & Virtualization Security

✓ *Spring*

- Ethical Hacking / Penetration Testing
- Cyber Threat Intelligence
- Governance, Risk & Compliance (GRC)
- Elective: IoT / Industrial Control Systems (ICS) Security

- *Year 4 – Integration, Leadership, and Emerging Areas*

✓ *Fall*

- Capstone Project I: Design & Planning
- Secure Architecture & System Design

✓ *Spring*

- Capstone Project II: Implementation & Presentation
- Cybersecurity Law, Policy, & Ethics
- Elective: Advanced Topics / Research Seminar Professional development
- Internship / Cooperative Experience Experiential learning

ABET does not list or impose these specific courses, however these courses and semester by semester yearly plan indicate the need for the required knowledge areas that must appear somewhere in the program. ABET recommends cybersecurity curricula cover five knowledge domains: data, software, system, human, and organizational security.

➢ *CAE Designations*

The need for standardized cybersecurity education is clear. To address this, understanding accreditation frameworks, especially the National Security Agency's (NSA) Centers of Academic Excellence (CAE) designations, becomes crucial. These designations serve as quality benchmarks and foster a cohesive approach to cybersecurity training across different institutions. Aspiring institutions must show they meet strict curricular and operational standards. Think alignment with the National Initiative for Cybersecurity Education (NICE), which defines necessary cybersecurity workforce skills (Tikanm Iäki et al., 2025). These designations are vital. They help create uniform educational outcomes, addressing existing program disparities and generally improving cybersecurity education quality (Jerman-Blazic A et al., 2024).The CAE program categorizes institutions by specialization, either Cyber Defense (CAE-CD) or Cybersecurity Research (CAE-R). This allows a sharper focus on specific study areas while keeping high educational standards across the board. Such categorization means graduates gain both foundational knowledge and skills specific to the workforce (Stavrou E et al., 2024). Furthermore, CAE designations stress practical experiences in programs. Students must engage in hands-on learning via labs and simulations mirroring real-world situations (Tay A et al., 2024).

➢ *Standards and Curriculum Guidelines.*

Crafting a strong cybersecurity curriculum—both for undergrads and those in graduate programs—hinges on clear standards and guidelines. Given the strong demand for cybersecurity pros across national security, industry, and even in academic circles, we need a systematic way to teach this stuff. Often, cybersecurity education suffers from a lack of standardization. This can create skills gaps in the workforce, and, frankly, puts national security at risk. But, by matching what we teach in school with recognized standards, colleges and universities can do a better job of getting grads ready to handle the ever-changing cyber threats out there. For example, the Accreditation Board for Engineering and Technology (ABET) and the National Security Agency (NSA), through its Centers of Academic Excellence program, are key players in setting quality benchmarks for cybersecurity education (Tikanm Iäki et al., 2025). They not only accredit programs, but also provide a yardstick for what should be taught, ensuring programs are useful and up-to-date. It's also important to include standards like the National Institute of Standards and Technology (NIST) Cybersecurity Workforce Framework, plus the ISO/IEC 27000 series for info security management. These push for a broad skill set, including things like risk management, incident response, and secure system design. All of this is super important for creating skilled cybersecurity people (Jerman-Blazic A et al., 2024). Furthermore, groups like the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) also contribute curriculum

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

guidelines tailored for computing, offering a well-rounded approach to integrating tech knowledge and skills (Stavrou E et al., 2024)(Tay A et al., 2024). The ongoing adjustments to these standards show how education and industry are intertwined, reflecting the diverse skills the cybersecurity workforce needs. Even with efforts to standardize cybersecurity education, there are still challenges. For instance, there can be tension between academic freedom and national standards. Schools might struggle to keep up with new threats while still being able to innovate and meet the specific needs of local industries (Yang Y et al., 2025). To keep pace with evolving industry standards and needs, it's essential to constantly assess and modify the curriculum. The most and top universally applied guidelines for standard and curriculum for University Programs are: 1) ABET, 2) ACM/IEEE CSEC2017, 3) NSA/DHS CAE-CD Knowledge Units, 4) NIST NICE Framework, and 5) ISO/IEC 27000-series.

➢ *Acquiring Cybersecurity Certifications.*

Preparing students to effectively tackle the cybersecurity field's intense demands requires integrating certifications into the curriculum—especially given rapidly changing threats and technologies. Cybersecurity certifications offer standardized ways to gauge a practitioner's skills, verifying expertise in areas like network security, ethical hacking, and even cloud security. Institutions can better align their programs with industry demands and desired professional skills by structuring curricula to emphasize recognized certifications (Tikanm Iäki et al., 2025). Certifications, such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), and Certified Information Security Manager (CISM), may enhance a graduate's employability by confirming technical skills and indicating a commitment to ongoing learning (Jerman-Blazic A et al., 2024). Students seeking these certifications while in degree programs often gain a more profound grasp of theoretical concepts, since practical application through certification training encourages engagement and improves knowledge retention (Stavrou E et al., 2024). Beyond just boosting job prospects, embedding certification requirements into coursework helps fill a gap in cybersecurity education: real-world practical experience. Institutions that strategically incorporate certification preparation into their coursework empower students to better navigate the complexities of cybersecurity, smoothing the transition from classrooms to professional roles (Tay A et al., 2024). Aligning curricula with certification standards further backs national frameworks like the NIST Cybersecurity Workforce Framework, highlighting defined knowledge, skills, and abilities (KSAs) crucial for cybersecurity roles (Avrahami Z et al., 2025). Pursuing certifications also sparks intrinsic motivation, driving students to engage more deeply with the material and enriching their broader learning journey (Yang Y et al., 2025). Balancing theoretical knowledge with practical certification training is paramount; graduates with relevant certifications often report greater job satisfaction and career growth than those without (Yogesh K Dwivedi et al., 2023).

Here is the recommended Learning Path by Academic Year:

Year 1–2 (Foundation)	CompTIA A+, Network+, Security+
Year 3 (Specialization)	CySA+, CEH, Cisco CyberOps, AWS Security
Year 4 (Integration & Leadership)	GSEC, CASP+, CISM, or CISSP
Graduate / Professional Level	CISSP, OSCP, CCSP, CRISC, or CISA

➢ *NIST & NICE Cybersecurity Workforce Framework*

Given the recognized need for consistent cybersecurity education, the NIST Cybersecurity Workforce Framework and the NICE Cybersecurity Workforce Framework act as key guides. They help shape what students learn and what skills they gain in both graduate and undergraduate programs. NIST, or the National Institute of Standards and Technology, has provided a strong base with its Cybersecurity Workforce Framework. This framework spells out the knowledge, skills, and abilities (KSAs) that cybersecurity pros need. It clearly defines roles and responsibilities, giving educators a plan to build their programs. By using common terms and definitions, NIST's framework encourages consistency across different schools, which is super important for closing the skills gap in cybersecurity, as shown in many studies (Tikanm Iäki et al., 2025), (Jerman-Blazic A et al., 2024).The NICE Cybersecurity Workforce Framework builds on this foundation. It goes deeper into the skills needed for different cybersecurity jobs. It stresses not just the technical skills, but also the soft skills and teamwork required to fight cyber threats (Stavrou E et al., 2024), (Tay A et al., 2024). The NICE framework also pushes for a complete understanding of cybersecurity, linking technology, methods, and how organizations work. This means programs should use real-world examples, like case studies and labs, to connect theory and practice. By working with industry, as the NICE framework suggests, schools can keep their courses up to date with the latest cybersecurity needs (Dubinsky V, 2024), (Avrahami Z et al., 2025). Using the NIST and NICE frameworks in courses also fits with the idea of focusing on what students can actually do after they graduate. Differences in funding, resources, and priorities can make it hard to implement these frameworks evenly. This can lead to differences in how good programs are and how ready students are (Yogesh K Dwivedi et al., 2023), (Bayer M et al., 2022).

Here are the yearly Cybersecurity courses plan from NIST and NICE:

- *Year 1: Foundations*

✓ Introduction to Programming & Computing Concepts
✓ Fundamentals of Networking & Operating Systems
✓ Introduction to Cybersecurity Concepts (CIA triad, threat types)
✓ Ethics, Legal & Society in Cybersecurity

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

- *Year 2: Core Technical Knowledge*

✓ Data Structures & Algorithms
✓ Systems Administration / OS & Virtualization
✓ Computer & Network Security Fundamentals
✓ Cryptography & Data Protection
✓ Human Factors, Social Engineering & Cyber-Awareness
✓ Elective / Free General Ed

- *Year 3: Applied & Specialized Security Topics*

✓ Incident Response & Digital Forensics
✓ Web & Application Security / Secure Software Development
✓ Cloud & Virtualization Security or Industrial Control Systems Security
✓ Governance, Risk & Compliance (GRC) in Cybersecurity
✓ Technical Writing / Communication for Cyber Professionals

- *Year 4: Integration, Leadership, Emerging Topics*

✓ Capstone Project in Cybersecurity (Team-based, real-world scenario)
✓ Secure System Architecture & Design (emerging tech: IoT, AI/ML)
✓ Cybersecurity Policy, Law & Strategy
✓ Internship / Practicum (optional)

➢ *ACM/IEEE Curriculum Guidelines in Computing Disciplines.*

When tackling the challenge of creating uniform cybersecurity courses for both undergrads and grads, it's crucial to have clear guidelines to make sure the education is both effective and relevant to industry. The Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) have come up with curriculum guidelines that act as key reference points for computer-related fields, including cybersecurity. These guidelines help schools shape their programs to meet industry demands and maintain high academic standards by providing a framework that highlights both basic and more advanced subjects. To be more precise, the ACM/IEEE Computer Science Curricula offers a step-by-step approach for adding not just technical skills but also important topics like ethics, legal issues, and the societal effects of technology (Tikanm Iäki et al., 2025). This comprehensive strategy is important because it helps people develop a deep understanding of the many different aspects of cybersecurity threats and defenses. It also gets graduates ready to handle the difficulties of today's digital world. Furthermore, the ACM/IEEE guidelines stress how important it is to build strong skills in areas like networking, system security, and software development, while also encouraging hands-on learning through labs and exercises (Jerman-Blazic A et al., 2024). By putting a focus on learning through doing, we can help close the gap between what students learn in the classroom and what they'll do on the job. As some studies have pointed out, educational programs stay current and effective when they regularly update their curricula based on the ACM/IEEE recommendations (Tay A et al., 2024).In addition to building technical skills, the ACM/IEEE framework helps create well-rounded graduates who can thoughtfully discuss issues like privacy, data protection, and cyber law by including subjects like ethics and policy (Dubinsky V, 2024).

Here are the recommended Four-Year Course Plan (ACM/IEEE-aligned)

- *Year 1 Foundations*

✓ Introduction to Programming / Computer Science I
✓ Introduction to Cybersecurity Fundamentals (covers cross-cutting concepts: confidentiality, integrity, availability, risk, adversarial thinking)
✓ Computer Systems & Architecture Fundamentals

- *Year 2 Core Technical Knowledge*

✓ Data Structures & Algorithms
✓ Networking Fundamentals
✓ Operating Systems & Systems Administration
✓ Secure Software Development
✓ Ethics, Law & Society in Cybersecurity

- *Year 3 Applied and Specialized Topics*

✓ Cryptography & Data Protection
✓ Application & Web Security
✓ Network Defense / Secure Communications
✓ Incident Response & Digital Forensics
✓ Governance, Risk & Compliance / Cyber Policy (Organizational Security + Societal Security)

- *Year 4 Integration, Capstone & Emerging Topics*

✓ Capstone Project in Cybersecurity
✓ Secure Systems Architecture & Design
✓ Emerging Topics in Cybersecurity
✓ Cybersecurity Leadership, Strategy & Ethics

III. UNDERGRADUATE CYBERSECURITY CURRICULUM STANDARDS

The education of future cybersecurity, particularly at the undergrad level—requires a well-thought-out strategy due to the growing complexity of cyber threats. It's crucial to establish solid curriculum standards. This not only addresses the rising need for experts in national security and different industries, but it also helps reduce skill gaps between different programs. A key part of any good cybersecurity undergraduate program? Comprehensive coverage of core skills like information security basics, how networks work, and software security protocols. This knowledge forms the foundation for students to build more specific skills, improving their chances of getting hired and their effectiveness in cybersecurity (Tikanm Iäki et al., 2025)(Jerman-Blazic A et al., 2024). Also, the curriculum needs to include ethical considerations, legal stuff, and policy issues related to cybersecurity. This makes sure grads understand the bigger picture when they use their technical skills. We can't stress enough how important this

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

understanding is, seeing as ethical mistakes or breaking the law can seriously hurt both individual careers and how an organization functions (Stavrou E et al., 2024)(Tay A et al., 2024).To really get students ready for real-world challenges, the curriculum must include practical learning, such as labs and technical exercises that mimic real cyber incidents. This hands-on approach not only improves problem-solving and critical thinking but also lets students deal with the ethical aspects of their work, encouraging a sense of professional duty (Dubinsky V, 2024)(Avrahami Z et al., 2025).

Undergraduate Cybersecurity Curriculum standard must cover cross-cutting cybersecurity concepts: confidentiality, integrity, availability (CIA), Data Security, Software Security, System Security. It also Must have an engaging capstone experience demonstrating mastery of cybersecurity concepts and practical skills. Curriculum should align with knowledge, skills, and abilities (KSAs) in relevant work roles. It must be based on ACM/IEEE Cybersecurity Curricula (CSEC2017). Recommended Curriculum Structure:

- Year 1: Foundations: programming, networking, discrete math, cybersecurity intro.
- Year 2: Core domains: operating systems, secure coding, cryptography, risks issues
- Year 3: Applied topics – incident response, cloud security, digital forensics, GRC.
- Year 4: Capstone & specialization – integration, leadership, research, internship.

➢ *Solid Comprehension of Ethics, Law, and Policies in Cybersecurity.*

For those stepping into the cybersecurity field, understanding the ethics, laws, and policies involved is super important. As digital systems become more a part of everyday life, cybersecurity decisions have implications that go way beyond just the technical stuff. They bring up ethical questions and deal with legal rules that affect both the public and private sectors. Getting a solid education in these areas means students can handle tough situations involving things like privacy, intellectual property, and following rules both here and abroad (Tikanm Iäki et al., 2025). This kind of knowledge is a must, especially with the rise in cybercrimes, so people need to know the legal consequences of what they do online. Programs that aim to teach ethics, law, and policy should use well-known guidelines like those from the National Institute of Standards and Technology (NIST) and the Cybersecurity Workforce Framework. That way, grads aren't just good at the tech stuff but also understand their responsibilities to society (Jerman-Blazic A et al., 2024). However, sometimes, ethics get left out of cybersecurity courses, which can create a gap between what's taught in class and what happens in the real world (Stavrou E et al., 2024).

➢ *Must have Labs and Technical Exercises and Programs.*

It's generally understood that a good cybersecurity education hinges on a solid pedagogical approach. However, just as important is integrating hands-on labs and technical exercises, ensuring a truly comprehensive grasp of the subject. Practical application complements what's learned in theory, letting students grapple firsthand with the complex cybersecurity challenges awaiting them in the real world. These meticulously designed labs, often mimicking actual networks and systems, allow students to apply their knowledge in a safe space. They can experiment, maybe even fail, but ultimately learn without risking real-world infrastructure. Research (Tikanm Iäki et al., 2025)(Jerman-Blazic A et al., 2024) suggests that this kind of immersive learning, through simulations and practical exercises, greatly improves how well students remember core skills and sharpens their critical thinking—both vital for a cybersecurity career.

Students in an undergraduate cybersecurity program should build and maintain hands-on skills yearly as follows:

- Year 1: Basic programming, network, and cybersecurity awareness labs.
- Year 2: System administration, secure coding, network defense, and cryptography labs.
- Year 3: Applied labs—penetration testing, digital forensics, cloud security, GRC.
- Year 4: Capstone integration, advanced security labs, emerging technology labs, internship.

IV. GRADUATE CYBERSECURITY CURRICULUM STANDARDS

The increasing number of cyber threats, together with significant technological advances, means we need to rethink the graduate cybersecurity education standards. Because cybersecurity professionals' skills vary, it's really important to set out graduate curriculum standards that cover both advanced topics *and* keep up with the field's ever-changing demands. Knowing a lot about cryptography and secure systems architecture is key; it’s the foundation for protecting sensitive data from more and more complex attacks (Tikanm Iäki et al., 2025). Also, grads should learn about cyber operations, digital forensics, and how artificial intelligence is being used in cybersecurity. This gives them the insights they need to see and respond to new threats (Jerman-Blazic A et al., 2024).The curriculum should also encourage cybersecurity research, so students can add to what we know and come up with new ways to tackle current issues (Stavrou E et al., 2024). This solid academic background should make sure learners not only meet the learning goals but can also quickly adjust to new cybersecurity rules and help create them as things change (Tay A et al., 2024). It's super important to balance the technical, managerial, and legal sides; students should learn how cybersecurity actions affect organizations and society in general (Dubinsky V, 2024).Getting cybersecurity certifications is becoming more and more important for this well-rounded education. They show the skills and knowledge that students gained in grad school (Avrahami Z et al., 2025). Institutions should make their curricula fit with established guidelines like the NIST Cybersecurity Workforce Framework and the ISO/IEC 27000 series for information security management. These guidelines help make sure things align with national standards (Yang Y et al., 2025). Plus, using the ACM/IEEE curriculum guidelines for computing can provide a good base that makes

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

graduate programs sound more instructive (Ramezanian S et al., 2024).

Graduate cybersecurity curriculum standards must:

- Educate improved and sophisticated technical, managerial, and societal domains.
- Incorporate and implement ABET, NICE, CAE-CDE, and CSEC2017 standards.
- Apply technical learning in hands-on labs, experimentation, and capstone/research experiences.
- Stress and teach ethics, policy, and risk management at an advanced level.
- Prepare graduates for professional, research, and leadership roles in cybersecurity.

➢ *Ability to Perform Research in Cybersecurity.*

Developing a robust cybersecurity curriculum necessitates instilling research skills in students, both at the undergraduate and graduate levels. This is vital for equipping them to meaningfully contribute to the field's ever-growing body of knowledge. This isn't just about academic prowess; it's a direct response to the cybersecurity world's urgent need for inventive approaches to combat new and evolving threats. Cybersecurity research is broad, encompassing topics like vulnerability assessments, threat modeling, and the creation of innovative cryptographic techniques – all crucial for strong cyberattack defenses (Tikanm Iäki et al., 2025). By incorporating research methodologies, students can engage in thorough analysis and practical experimentation, promoting a culture of curiosity and innovation (Jerman-Blazic A et al., 2024). A solid grasp of empirical research methods and data gathering is essential; it allows students to expand on current cybersecurity research and explore new frontiers (Stavrou E et al., 2024). This initial exposure sets the stage for the heightened research expectations of graduate programs. There, the focus shifts to applying theoretical frameworks to tangible cybersecurity problems. Graduate students should not only absorb existing knowledge but also generate original research that could shift industry norms or influence policy (Tay A et al., 2024). Creating research opportunities in universities often demands significant resource and infrastructure investment.

Here are some areas in Cybersecurity that a graduate student can conduct research in depth:

- *Network & Infrastructure Security:*

✓ Next-generation firewalls, intrusion detection/prevention systems (IDS/IPS)
✓ Software-defined networking (SDN) security
✓ 5G/6G wireless network security

- *Cloud, Virtualization & Distributed Systems Security*

✓ Cloud-native security (AWS, Azure, GCP)
✓ Container & Kubernetes security
✓ Virtual machine escape and hypervisor hardening

- *Cryptography & Applied Security*

✓ Post-quantum cryptography

- *Secure Software Engineering*

✓ Secure software development lifecycle (SDLC)
✓ Skills/Tech: Static/dynamic code analysis, fuzzing, DevSecOps tools

- *Penetration Testing & Offensive Security*

✓ Advanced exploitation techniques
✓ Red teaming frameworks

- *Digital Forensics & Incident Response*

✓ Memory forensics and malware analysis
✓ Cloud forensics

- *Artificial Intelligence & Machine Learning in Cybersecurity*

✓ Threat detection using machine learning

➢ *Ability to Follow Cybersecurity Policies and Devise New Ones.*

One core element of building strong cybersecurity programs lies in developing the ability to not just follow cybersecurity policies, but also to come up with new ones that keep pace with our rapidly changing digital world. This dual requirement is key, as those in the field must be able to work with existing policies while also spotting weaknesses that need fresh solutions. A basic need for this is a solid grasp of current cybersecurity ideas, along with the regulatory, ethical, and legal rules that affect how tech is used (Tikanm Iäki et al., 2025), (Jerman-Blazic A et al., 2024). Grad students, especially, should study frameworks from groups like the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA), which give essential advice for creating and putting policies in place (Stavrou E et al., 2024), (Tay A et al., 2024).But, coming up with strong policies shouldn't just be about theory; putting ideas into practice is super important. For example, simulated scenarios and case studies can help us discuss how to make good cybersecurity policies that tackle new threats, like those from artificial intelligence and machine learning (Dubinsky V, 2024), (Avrahami Z et al., 2025). Also, because cybersecurity is increasingly tied to privacy and ethics, students should be able to suggest policies that not only lower risks but also stick to ethical standards (Yang Y et al., 2025), (Ramezanian S et al., 2024). By working with policy analysis and creation in their courses, students can start to see how tech choices impact public safety, data privacy, and even financial security.

Here are some policies that need to be updated or rewritten: Data Privacy and Protection Policies, Cloud and Virtualization Security Policies, Incident Response & Cybersecurity Governance Policies, Risk Management and

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

Compliance Policies, and Cybersecurity Awareness and Training Policies.

V. DIFFICULTIES IN ACHIEVING STANDARDIZATION

It's generally understood that standardizing cybersecurity curricula presents complex issues for educational institutions. Balancing academic freedom with national standards isn't always easy and can sometimes slow down the development of comprehensive programs. Institutions value being able to innovate and customize courses for local needs, but too much flexibility can lead to inconsistent educational results, making it harder to establish uniform standards. As studies have shown, institutions often prioritize their own educational philosophies, which leads to different interpretations of necessary skills and knowledge, and makes overall standardization difficult (Tikanm Iäki et al., 2025)(Jerman-Blazic A et al., 2024).The cybersecurity field is constantly changing, with new breaches and technological advances requiring frequent curriculum updates to stay current with threats and industry standards. If programs can't adapt quickly enough, students may not be adequately prepared, and the institution might seem out of touch, since its programs won't reflect industry best practices (Stavrou E et al., 2024)(Tay A et al., 2024). These changes demand continuous improvement of course content and a formal approach to curriculum development, agile enough to incorporate new trends while maintaining academic standards.

There are reasons why there are difficulties in achieving standardization in Curricula for Cybersecurity education and some are: ongoing Cyber Threat and its sophistication, Lack of agreement on Core Knowledge Areas, difference and gaps in Institutional Resources, Differences in Accreditation and Regulatory Requirements, and Differences in Industry Expectations, Hands-On Experience Standardization, and Faculty Expertise and Training Gaps

- *Challenges of Incorporation of Academic Freedom with National Standards.*

The governance of cybersecurity programs in education involves navigating tricky terrain, particularly when balancing academic freedom with the need to meet national standards. Academic freedom, a key principle in higher education, lets educators explore, create, and change curricula to best fit their schools and student needs. It's crucial for encouraging critical thinking and new ideas, allowing teachers to tailor their lessons to current issues and improve students' analytical skills in the fast-changing cyber world (Tikanm Iäki et al., 2025). However, national standards can sometimes cause problems; their strictness might limit creativity, making it harder for educators to quickly respond to evolving cybersecurity threats. Trying to meet these standards while also supporting faculty independence can cause conflicts that hinder the goals of educational institutions (Jerman-Blazic A et al., 2024). Also, aligning curricula with national standards raises questions about whether current frameworks adequately address the specific, complex needs of cybersecurity education. Groups like the National Institute of Standards and Technology (NIST) offer frameworks, but these should be flexible enough to accommodate different institutional goals and philosophies (Stavrou E et al., 2024). While the National Cybersecurity Workforce Framework outlines important skills, knowledge, and abilities, educators should have the flexibility to adjust their focus based on their institution's priorities, whether it's technical expertise, policy work, or risk management (Tay A et al., 2024). Finding this balance becomes harder when considering the various metrics used by accrediting bodies like ABET and CAE to assess program effectiveness (Dubinsky V, 2024). Resource disparities among institutions further complicate this dilemma, exacerbating the challenges of curriculum standardization. Not all schools have the same access to advanced technology, skilled faculty, or funding, which can greatly affect their ability to deliver education that aligns with national standards (Avrahami Z et al., 2025). As a result, a uniform approach to cybersecurity education based solely on national benchmarks might unintentionally reinforce existing inequalities.

- *Difference and Gaps in Available Resources Among Institutions.*

The varied resources available across different institutions can really throw a wrench into setting up a standard cybersecurity curriculum. It's obvious that this creates a noticeable gap in how well and how easily people can access cybersecurity education. You see, the amount of money universities put into their cybersecurity programs differs quite a bit. Some have impressive, up-to-date tech and facilities, while others struggle to even get the basics for teaching and setting up labs. This difference doesn't just impact the hands-on training students get; it also leads to some big differences in what students learn at different schools (Tikanm Iäki et al., 2025). In conclusion, the resources differing across institutions amplify the difficulties in developing a standardized cybersecurity curriculum. To get past these gaps, we need a group effort that focuses on working together, finding new funding solutions, and keeping the quality of education consistent. This will ensure that all students get the skills-based education they need to succeed in the fast-changing world of cybersecurity (Mukherjee M et al., 2024)(Sutherland E et al., 2023). Addressing this issue is paramount not only for the sake of educational equity but also for the essential security of our society at large (Shuroug A Alowais et al., 2023)(Allioui H et al., 2023).

VI. RECOMMENDATIONS

To truly boost cybersecurity education, we need some key steps that consider insights from schools, businesses, and the government. The National Institute of Standards and Technology (NIST) Cybersecurity Workforce Framework (NICE) should be used in all schools. This gives us a guide for the skills people need, which helps colleges create good programs (Tikanm Iäki et al., 2025). Also, it’s important for schools and companies to work together, ensuring programs keep up with new cyber threats (Jerman-Blazic A et al., 2024). Sharing knowledge and resources can lead to programs that teach the basics and encourage new ways of solving problems (Stavrou E et al., 2024). Getting enough

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

money for teachers and labs is also vital. Investing in teacher training keeps them up to date, so they can create lessons based on real-world situations (Tay A et al., 2024). Modern labs let students get hands-on experience, which is crucial for learning cybersecurity skills (Dubinsky V, 2024). Focusing on both teachers and resources really improves the quality of education. It's also imperative to regularly revise and update programs to reflect what's currently happening in the field. Educational institutions need to formalize processes for reviewing and improving curricula, based on research, tech innovation, and industry standards (Avrahami Z et al., 2025). Keeping curricula up to date makes sure students learn the right skills to succeed in their careers (Yang Y et al., 2025). Being responsive to change helps both students and the school's reputation. Accreditation is necessary for cybersecurity programs to ensure standardization and credibility. Groups like the Accreditation Board for Engineering and Technology (ABET) and Centers of Academic Excellence (CAE) evaluate programs to see if they meet educational requirements (Ramezanian S et al., 2024). Seeking accreditation pushes schools to meet academic and industry standards, improving the rigor of what they offer (Segate RV, 2024). Getting certifications like Certified Information Systems Security Professional (CISSP) or Certified Ethical Hacker (CEH) gives students credentials that boost their job chances (Yogesh K Dwivedi et al., 2023). These certifications show students and teachers the importance of covering relevant material. Lastly, it's important to even the playing field between institutions so that all have a fair shot to create top-notch cybersecurity offerings.

- *Apply NIST NICE Framework Across All Levels.*

For a cohesive and thorough educational groundwork, integrating the NIST NICE Framework across cybersecurity curricula remains quite essential. The National Initiative for Cybersecurity Education (NICE) Framework supplies a structured method. This method delineates the required knowledge, skills, and abilities (KSAs) needed for the various cybersecurity roles. By mapping curricula with the NICE Framework, educational institutions are better positioned to confirm that their programs align with national standards. They also can better align with workforce needs, thereby addressing the increasing need for skilled cybersecurity pros in areas like national security, industry, and academia (Tikanm Iäki et al., 2025). The framework's core competencies also help to connect academic learning to practical application, ensuring grads are not just theoretically sound, but also skilled in applying those skills in real-world scenarios (Jerman-Blazic A et al., 2024). When thinking about undergraduate programs, adhering to the NICE Framework makes it easier to incorporate necessary technical skills. Think network security, systems security, and even ethical hacking. However, it also emphasizes critical soft skills, like problem-solving, and sometimes overlooked ethical decision-making (Stavrou E et al., 2024). Cybersecurity threats are consistently evolving; educational content must evolve, too. NICE-aligned maps can allow programs to remain relevant. This is achieved by updating essential KSAs that reflect current industry needs and emerging challenges (Tay A et al., 2024). Crucially, the framework assists in creating measurable learning outcomes, vital for both program assessment and, you guessed it, accreditation processes, such as those mandated by ABET and NSA's Center for Academic Excellence Designations (Dubinsky V, 2024).At the graduate level, the NICE Framework can inform the development of advanced curricula.

- *Constant Cooperation between Academia, Industry, and Government.*

The cybersecurity field is constantly changing, which means we need strong partnerships between universities, businesses, and government agencies. These partnerships are key to training skilled professionals who can handle new challenges. Studies show that when these groups work together, education becomes more effective because the curriculum stays up to date with real-world needs and new technologies (Tikanm Iäki et al., 2025). Universities can give students a much better understanding of how cybersecurity works in practice by connecting what they learn in the classroom with the experiences of industry experts. One good way to do this is through internships, co-op programs, and joint research projects. This way, students get to work on real projects that address current threats and weaknesses in organizations (Jerman-Blazic A et al., 2024). Not only does this make learning more interesting, but it also prepares students to deal with the complexities of modern cybersecurity. Industry input is also important for making sure that the curriculum covers what the job market needs. For instance, industry professionals can tell educators if the courses being offered are relevant and if graduates have the right skills that employers are looking for (Stavrou E et al., 2024). Working with government organizations is also crucial, especially when setting standards for cybersecurity programs in higher education. Programs like the National Security Agency's Centers of Academic Excellence serve as a good example of how to match educational goals with national security needs. These programs make sure that graduates are well-trained to support both public and private cybersecurity efforts (Tay A et al., 2024). These partnerships can help to regularly check if the curriculum is still relevant and effective and ensure that the course content keeps up with the rapidly changing threat landscape. Moreover, these kinds of collaborations can create research opportunities that help us better understand cybersecurity. When universities, private companies, and government agencies work together on research, it can lead to valuable insights and innovations that shape effective cybersecurity strategies. Here is the main need for Coordination and cooperation between academia, industry, and government:

- Academia: Teach and equip students with base knowledge, structured curricula, labs, and theoretical comprehension.
- Industry: Supplies hands-on labs, real-world projects, mentorship, and latest technology exposure.
- Government: Ensures policy, legal, regulatory, and national security perspectives are integrated, plus internship opportunities in public sector agencies.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

➢ *Proper and avid funding for faculty development and lab infrastructure*.

In the ongoing effort to build a solid cybersecurity curriculum, we can't stress enough how vital it is to put significant funding into faculty development and lab infrastructure. The cybersecurity world keeps changing, with new threats and tech popping up all the time. That means our teachers need to be experts in their fields and keep learning to stay sharp. If we fund them well, they can attend workshops, conferences, and get more certifications. This makes them better teachers and ensures they're teaching the latest and most important stuff (Tikanm Iäki et al., 2025). Plus, faculty with good support can add to academic research, pushing the field forward and encouraging innovation in our schools (Jerman-Blazic A et al., 2024).State-of-the-art labs are also super important for hands-on learning in cybersecurity education. They let students use what they learn in real-world situations, like ethical hacking, digital forensics, and dealing with incidents (Stavrou E et al., 2024). Studies show that this kind of experience really helps students understand cybersecurity principles. And that better prepares them for the challenges they'll face when they start working (Tay A et al., 2024). So, we need to fund not just the upkeep of our labs but also upgrades to keep up with the latest tech. This means investing in simulation tools, network setups, and advanced threat assessment systems to give students a realistic space to develop their skills (Dubinsky V, 2024).Beyond just the physical stuff, money plays a big role in getting faculty from different departments to work together. When schools help create a collaborative environment, they can bring insights from fields like law, ethics, and tech into the cybersecurity curriculum (Avrahami Z et al., 2025).

➢ *Recommendations for Future Curriculum Development*

Given the pressing need for capable cybersecurity experts in today's fast-changing world, curriculum development must be agile and in line with industry norms. It should also promote cooperation among schools, businesses, and government bodies:

- Using a detailed framework like the NIST NICE Cybersecurity Workforce Framework can help lay the groundwork for curricula that teach essential cybersecurity skills (Tikanm Iäki et al., 2025). These recommendations also highlight the need for partnerships among different groups, ensuring that educational programs keep up with the latest cybersecurity threats and tech breakthroughs.
- Consistent talks between schools and industry leaders will help curricula include current best practices and real-world insights, improving student learning (Jerman-Blazic A et al., 2024).It is also essential to have adequate funding for faculty growth and lab equipment, which are crucial for giving students hands-on experience (Stavrou E et al., 2024).
- It is also important to align curriculum content with national and international standards from groups like ABET and CAE; these act as benchmarks for educational quality and job readiness (Dubinsky V, 2024). Also, programs should be regularly assessed, including input from working pros, to ensure learning objectives remain current and thorough (Avrahami Z et al., 2025).Curricula must also stress ethics, laws, and policies, given the rising complexity of cyber threats.
- Furthermore, specialized tracks in both undergrad and graduate programs should build skills in new areas like AI in cybersecurity, digital forensics, and incident response (Ramezanian S et al., 2024). This targeted approach will ensure that graduates are ready to tackle cybersecurity challenges and fill crucial job openings (Segate RV, 2024). Recommendations should also encourage earning recognized cybersecurity certifications, which are seen as marks of quality and can help job seekers stand out (J R K Bokau et al., 2024). These certifications will boost graduates' employability and show employers their skills. Curricula should also include ISO/IEC 27000 family guidelines, which focus on managing sensitive data and reducing risks (Yogesh K Dwivedi et al., 2023). Using these frameworks will create a more organized cybersecurity education, aligning student skills with global benchmarks.
- Finally, it is important to promote a culture of innovation and ongoing improvement in the cybersecurity curriculum. Schools should encourage lifelong learning and adaptability among faculty and students, recognizing that ongoing education is key in the face of new technologies and threats (Bayer M et al., 2022). By following these recommendations, educational programs can produce cybersecurity professionals who have the necessary skills, ethics, and resilience to handle the complexities of this important field. This proactive curriculum development will improve the quality and relevance of cybersecurity education and significantly contribute to national and global cybersecurity efforts (Sithara H P W Gamage et al., 2022).

VII. CONCLUSION

When we consider cybersecurity education, it's clear that having some kind of shared framework is important. It's about getting people ready to deal with the ever-growing challenges in this field. Graduate and undergraduate programs should really be aiming to fix the educational gaps we see now. These gaps can lead to a shortage of skilled people and make things less efficient at work (Tikanm Iäki et al., 2025). Industries, security agencies, and schools all need more cybersecurity experts, so it's crucial for educational institutions to keep up. They should align their programs with standards like ABET accreditation and CAE designations (Jerman-Blazic A et al., 2024). These things give guidelines for setting up courses, but also make sure graduates have the necessary skills to work in different cyber environments. Besides accreditation groups, things like the NIST & NICE Cybersecurity Workforce Framework help define the skills needed for the job (Stavrou E et al., 2024).Putting standardized curricula into action helps us see what skills are needed at different education levels. Undergrads should get a good base in areas like information security, networking, and legal policies (Tay A et al., 2024). Moving into graduate studies, students are expected to know more about cryptography and secure systems, and how tech changes

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar896

affect things (Dubinsky V, 2024). Also, developing solid problem-solving and critical thinking skills is key. It helps students handle the real-world problems they'll face later (Avrahami Z et al., 2025). Practical labs and exercises really boost the learning experience too.

REFERENCES

[1]. Ilkka Tikanmäki, J. Rajamäki (2025) Research in Education: Case Cybersecurity Project. European Conference on Research Methodology for Business and Management Studies. doi: https://www.semanticscholar.org/paper/be29d4f72bfc1647ee05fdcdaa63cbe831ba9e71

[2]. Andrej Jerman-Blazic, B. Jerman-Blazic (2024) Teaching and learning cybersecurity for European youth by applying interactive technology and smart education. Volume (30), 9093-9120. Educ. Inf. Technol. doi: https://www.semanticscholar.org/paper/ebbce21ca33f4d809c4cc5f1766b566040802501

[3]. Eliana Stavrou, Andriani Piki (2024) Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity. Volume(32), 523-541. Inf. Comput. Secur.. doi: https://www.semanticscholar.org/paper/93128656734aeed2ef920566992be7e43e188101

[4]. Albert Tay, Sebastian M Hayes, Drew Wilson, Emmie Hall, Dallin Kaufman (2024) Gamified Cybersecurity Education Through the Lens of the Information Search Process: An Exploratory Study of Capture-the-Flag Competitions [Research-in-Progress]. Issues in Informing Science and Information Technology. doi: https://www.semanticscholar.org/paper/88e889d975b290bb9cc54512d32661d7069888cb

[5]. Vitaliy Dubinsky (2024) TRAINING OF COMPUTER SCIENCE TEACHERS FOR THE FORMATION OF CYBERSECURITY SKILLS IN STUDENTS: ACTUALIZATION OF PROBLEMS AND THEIR POSSIBLE SOLUTIONS. Education. Innovation. Practice. doi: https://www.semanticscholar.org/paper/f406cc08db2b46d465aa7d1cb4e5adb34ffd0cc0

[6]. Zafrir Avrahami, M. Zwilling, Chen Hajaj (2025) Leveraging OSINT for Advanced Proactive Cybersecurity: Strategies and Solutions. Volume(13), 154229-154250. IEEE Access. doi: https://www.semanticscholar.org/paper/fe8b3e9d578c6da327e9fca369cdc98f6e5b1d25

[7]. Yimei Yang, Jinping Liu, Yujun Yang (2025) Research on China's Innovative Cybersecurity Education System Oriented Toward Engineering Education Accreditation. Information. doi: https://www.semanticscholar.org/paper/543b8e7d53661255f3bdfcb7b405a59c147f1d47

[8]. Sara Ramezanian, Valtteri Niemi (2024) Cybersecurity Education in Universities: A Comprehensive Guide to Curriculum Development. Volume(12), 61741-61766. IEEE Access. doi: https://www.semanticscholar.org/paper/7522ce908e33d64bcf48ccf519082ec7ff597c3f

[9]. Riccardo Vecellio Segate (2024) Drafting a Cybersecurity Standard for Outer Space Missions: On Critical Infrastructure, China, and the Indispensability of a Global Inclusive Approach. Volume(11), 345 - 375. Journal of Asian Security and International Affairs. doi: https://www.semanticscholar.org/paper/468dffedea0514679d901afe55c31fca7d95ce11

[10]. Yogesh K. Dwivedi, Nir Kshetri, Laurie Hughes, Emma Slade, Anand Jeyaraj, Arpan Kumar Kar, Abdullah M. Baabdullah, et al. (2023) Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. Volume(71), 102642-102642. International Journal of Information Management. doi: https://doi.org/10.1016/j.ijinfomgt.2023.102642

[11]. Markus Bayer, Marc–André Kaufhold, Christian Reuter (2022) A Survey on Data Augmentation for Text Classification. Volume(55), 1-39. ACM Computing Surveys. doi: https://doi.org/10.1145/3544558

[12]. Sithara H. P. W. Gamage, Jennifer R. Ayres, Monica Behrend (2022) A systematic review on trends in using Moodle for teaching and learning. Volume(9). International Journal of STEM Education. doi: https://doi.org/10.1186/s40594-021-00323-x

[13]. Rajendra Raj, Mihaela Sabin, John Impagliazzo, David Bowers, Mats Daniels, Felienne Hermans, Natalie Kiesler, et al. (2021) Professional Competencies in Computing Education. doi: https://doi.org/10.1145/3502870.3506570

[14]. Mamdouh Alenezi (2021) Deep Dive into Digital Transformation in Higher Education Institutions. Volume(11), 770-770. Education Sciences. doi: https://doi.org/10.3390/educsci11120770

[15]. Madhav Mukherjee, Ngoc Thuy Le, Yang-Wai Chow, Willy Susilo (2024) Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. Volume(15), 117-117. Information. doi: https://doi.org/10.3390/info15020117

[16]. Eric Sutherland, Rishub Keelara, Samuel Eiszele, June Haugrud (2023) Fast-Track on digital security in health. OECD health working papers. doi: https://doi.org/10.1787/c3357f9f-en

[17]. Shuroug A. Alowais, Sahar S. Alghamdi, Nada Alsuhebany, Tariq Alqahtani, Abdulrahman Alshaya, Sumaya N. Almohareb, Atheer Aldairem, et al. (2023) Revolutionizing healthcare: the role of artificial intelligence in clinical practice. Volume(23). BMC Medical Education. doi: https://doi.org/10.1186/s12909-023-04698-z