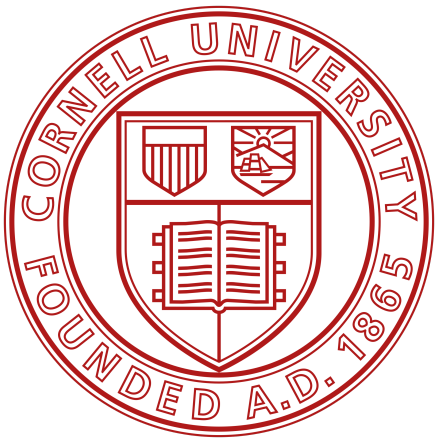
International Strategies for Early Cybercrime Prevention: A Comparative Analysis of the United States and European Nations

Cynthia Tan

Cornell University
Cornell Brooks School Tech Policy Institute
Federal Bureau of Investigation
National Cyber-Forensics and Training Alliance



NCFTA

Abstract

As the digital landscape continues to expand, cybercrime has become a significant global issue, requiring more effective and coordinated responses. This paper explores the growing problem of youth involvement in cybercrime, emphasizing the need for early prevention strategies. Numerous studies underscore the financial and security impacts of cyberattacks, which are expected to cost the global economy $9.5 trillion annually by 2024. Early engagement in hacking is prevalent among youth, with many starting in their teenage years or earlier. Countries such as the Netherlands, the United Kingdom, and Finland have developed successful programs, such as ethical hacking initiatives and educational interventions, to divert young individuals from illegal activities. These efforts have shown significant reductions in youth involvement in cybercrime.

This paper is a comparative study that utilizes global cybersecurity indices, including the Global Cybersecurity Index (GCI), Cybersecurity Preparedness Index (CPI), and Cyber Risk Index (CRI), to evaluate the United States' cybersecurity efforts against selected European countries. The urgency of this issue is highlighted by a recent report from the Department of Homeland Security's Cyber Safety Review Board, which recommended that Congress explore funding juvenile cybercrime prevention programs to help steer young people away from illegal hacking and other online crimes.

The findings show that while the United States performs strongly in areas like legal measures and technical capabilities, it lags behind European countries in youth-focused cybercrime prevention. Countries like the Netherlands and the UK, which have implemented comprehensive ethical hacking programs and early intervention initiatives, demonstrate significantly lower rates of youth cybercrime involvement. The paper identifies best practices from these countries that could inform the development of similar programs in the U.S. Through early intervention and ethical education, the U.S. can mitigate future cybersecurity risks, reduce youth hacking by up to 60%, and foster a new generation of cybersecurity professionals.

Introduction

In today's digitally connected world, cybercrime has become a widespread global issue that still lacks a sufficiently developed, coordinated response. Numerous studies have documented the detrimental effects of hacking on the global economy and security, highlighting the urgent need for a serious strategy towards early youth prevention. Cyberattacks cost the U.S. economy billions annually, and the increasing sophistication of these attacks poses a growing threat to national security (Vojinovic, 2023[1]; FBI, 2023[2]). The global cost of cybercrime is projected to reach $9.5 trillion annually by 2024, underscoring its severe economic impact (Morgan, 2023[3]).

---

[1] Vojinovic, I. (2023, July 14). More Than 70 Cybercrime Statistics - A $6 Trillion Problem. DataProt. Retrieved from https://dataprot.net/statistics/cybercrime-statistics/

[2] FBI. (2023). Internet Crime Report 2023. Internet Crime Complaint Center. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[3] Morgan, S. (2023, October 25). Cybercrime to cost the world $9.5 trillion annually in 2024. Cybersecurity Ventures. Retrieved from

Research indicates that many hackers start their activities at a young age, with several reports suggesting that a significant portion of cybercriminals begin hacking during their teenage years or earlier (Daunton, 2023[4]; Gregory, 2022[5]). Early prevention efforts can reduce hacking incidences significantly, with some studies suggesting reductions by up to 60% (Stouffer, 2022)[6].

Primary reasons for children getting involved in hacking include curiosity, peer influence, and the desire for social recognition or financial gain. Ethical hacking programs in countries such as the Netherlands provide a constructive outlet for children interested in cyberspace. These programs allow them to safely pursue their intellectual curiosity while enhancing cybersecurity by identifying and addressing vulnerabilities. For example, the Netherlands' Coordinated Vulnerability Disclosure (CVD) policy actively encourages hackers to find and report security weaknesses, providing a legal and ethical framework for their activities (Noordegraaf & Kranenbarg, 2023)[7]. Such initiatives have been successful in redirecting potential cybercriminals towards ethical hacking practices, thereby improving cybersecurity for both private and public interests. Other countries have also developed similar successful programs. In the United Kingdom, the National Crime Agency's Cyber Choices program educates young people about the legal and ethical aspects of cybersecurity, offering pathways to legitimate careers through mentorship and workshops (Daunton, 2023)[8]. Similarly, Finland's Cybercrime Exit Project targets young people aged 12 to 25, teaching them the difference between legal and illegal hacking and diverting them away from criminal activities (Aiken et al., 2016)[9].

It is of utmost importance for the United States to pursue youth cybercrime prevention programs due to the significant financial and security implications of cybercrime. By learning from successful international models, the U.S. can develop effective strategies to mitigate the risk of youth involvement in cybercrime. This approach will help cultivate a new generation of cybersecurity professionals, thereby enhancing national security and contributing to the long-term prosperity of the economy. Investing in these programs now will ensure a more secure and resilient future.

This paper aims to bridge the gap in knowledge necessary to make the development of youth cybercrime prevention programs possible. This comes with great urgency from a report by the

---

https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/#:~=A%20breakdown%20of%20global%20cybercrime,%24182.5%20billion%20USD%20a%20week

[4] Daunton, N. (2023, June 12). Are the kids alright? How European authorities want to tackle child hacking. Euronews. Retrieved from https://www.euronews.com/next/2023/06/12/are-the-kids-alright-how-european-authorities-want-to-tackle-child-hacking

[5] Gregory, J. (2022, August 30). Why teens become cyber criminals. Security Intelligence. Retrieved from https://securityintelligence.com/articles/why-teens-become-cyber-criminals/

[6] Stouffer, C. (2022, September 1). 115 cybersecurity statistics + trends to know in 2024. Norton. Retrieved from https://us.norton.com/blog/emerging-threats/cybersecurity-statistics

[7] Noordegraaf, J. E., & Kranenbarg, M. (2023, October 11). Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. Criminology, 61(1), 121-145. doi:10.1111/1745-9133.12650

[8] Daunton, N. (2023, June 12). Are the kids alright? How European authorities want to tackle child hacking. Euronews. Retrieved from https://www.euronews.com/next/2023/06/12/are-the-kids-alright-how-european-authorities-want-to-tackle-child-hacking

[9] Aiken, M., Davidson, J., & Amann, P. (2016, October). Youth pathways into cybercrime. Europol. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/pathways-white-paper.pdf

Department of Homeland Security's Cyber Safety Review Board[10] recommending that Congress explore funding juvenile cybercrime prevention programs that could help steer young people away from illegal hacking and other online crimes.' This recommendation was made as part of an investigation last year into Lapsus$, a teenage hacking group known for its attacks on major companies like Microsoft, Nvidia and Rockstar Games.

Literature Review

While cybercrime as a whole has been extensively studied, research specifically focused on youth involvement in cybercrime remains relatively scarce. This gap can be attributed to the anonymity that the cybercrime environment offers, making it difficult to identify and track young offenders. Additionally, youth prosecution records are often sealed, limiting access to detailed information on cases involving young individuals. These factors create significant challenges for researchers attempting to study youth cybercrime patterns and develop targeted interventions.

Young hackers are often drawn to cybercrime through a mix of intellectual curiosity, social influences, and the promise of financial gain, yet the pathways they follow into these activities and the factors that differentiate them from adult cybercriminals are not well understood. This gap in the literature is particularly concerning given that early intervention has been shown to be one of the most effective strategies for diverting young individuals away from illegal activities.

International responses to youth cybercrime prevention have varied, with some countries developing comprehensive and innovative programs that not only divert potential offenders but also channel their skills into ethical hacking and cybersecurity careers. For instance, European nations in the European Union Agency for Law Enforcement Cooperation, known as Europol, such as the Netherlands and the United Kingdom have made significant strides in implementing such programs, offering a blueprint for how to engage young people constructively in the cybersecurity field. However, the United States has yet to develop a similarly cohesive and effective approach, which has resulted in a missed opportunity to cultivate young talent while reducing the economic and security risks posed by cybercrime.

This literature review examines the current state of research on youth cybercrime and explores existing prevention programs across various countries. By analyzing these international initiatives and the factors influencing youth participation in cybercrime, this review seeks to identify best practices that could inform more effective youth prevention programs in the United States by looking at existing programs that are effective. Additionally, the review will highlight critical gaps in the literature and propose areas for further investigation to advance the understanding of youth cybercrime.

1. Typical Hacker Profile

[10] Cybersecurity and Infrastructure Security Agency. (2023). Review of the attacks associated with Lapsus$ and related threat groups. Retrieved from https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf

Firstly, to understand the cybercrime space, understanding the typical profile of a hacker is crucial for developing effective prevention strategies. In this paper, we adopt Europol's definition of a hacker: "Individuals who use their technical skills to gain unauthorized access to computer systems, networks, or data. This access is typically used to exploit system vulnerabilities, steal information, or disrupt services" (Europol, 2023).

Hackers often share common traits shaped by psychological, social, and environmental factors. Research indicates that many young hackers are highly intelligent and driven by a strong curiosity about technology and how systems function. This natural curiosity frequently leads to exploratory behaviors, starting with innocuous activities like modifying video games or investigating system vulnerabilities purely for fun. However, without proper guidance or an ethical framework, these behaviors can escalate into illegal cyber activities (Aiken et al., 2024; Youth Lab, 2023)[11]. Understanding these tendencies and addressing them through early intervention and ethical education is critical in preventing youth from progressing into more serious cybercriminal behavior.

1.1 Demographics and Background

Hackers tend to be young, with many beginning their activities during their teenage years or even earlier. According to a Tufin survey, one in six teenagers in New York has admitted to hacking, with most reporting that they rarely get caught. This highlights the early age at which many individuals begin engaging in cyber activities, often driven by curiosity and experimentation (Tufin, 2023)[12]. The anonymity and accessibility of online hacking tools allow teenagers to explore cybercrime with minimal risk of immediate consequences, further contributing to their involvement at a young age.

Research consistently shows that young males significantly outnumber females in youth cybercrime. However, female participation has been on the rise in recent years. Many of these individuals come from middle- to upper-class backgrounds, with early access to technology like computers and the internet. This early access allows them to develop technical skills that surpass those of their peers, which can lead to experimentation with system vulnerabilities and eventually escalate into cybercriminal activities (University of East London, 2022; Dedovic, 2020)[13][14].

---

[11] Aiken, M., Davidson, J. C., Walrave, M., Ponnet, K. S., & Farr, R. R. (2024). Intention to hack? Applying the Theory of Planned Behaviour to youth criminal hacking. *Forensic Sciences, 4*(1), 24-41. https://doi.org/10.3390/forensicsci4010003
Youth Lab. (2023). Hacker culture: The young world of cybercrime. *The Youth Lab*. Retrieved from https://www.theyouthlab.com/insights/hacker-culture-the-young-world-of-cybercrime

[12] Tufin. (2023). *Tufin survey finds one in six New York teenagers hack and rarely get caught*. https://www.tufin.com/pr/tufin-survey-finds-one-in-six-new-york-teenagers-hack-and-rarely-get-caught
[13] University of East London. (2022). *Two thirds of European youth involved in cybercrime*. https://www.uel.ac.uk/about-uel/news/2022/december/two-thirds-european-youth-involved-some-form-cybercrime-online-risk-taking
[14] Dedovic, Y. (2020). *Cybercrime: Internet erodes teenage impulse controls*. ScienceDaily. https://www.sciencedaily.com/releases/2020/01/200121112915.htm

Additionally, young hackers often report feelings of social disconnection or alienation, which drive them to seek validation in online communities. These digital spaces, where their technical skills are acknowledged and rewarded, create a sense of belonging and further reinforce their involvement in illegal cyber activities (Muncaster, 2022)[15].

1.2 Psychological Traits

Young hackers often exhibit a combination of psychological traits, including high cognitive ability and a natural curiosity about technology. For many young people, these traits are initially cultivated through gaming. Online gaming environments often reward players for strategic thinking, problem-solving, and exploiting in-game systems to gain an advantage. This culture of exploration and optimization can extend into hacking, as young individuals seek to understand and manipulate both gaming systems and broader technological environments (Aiken et al., 2024). Additionally, the competitive nature of gaming can foster risk-taking behavior and a desire for social recognition within gaming communities. Adolescents, who are particularly susceptible to peer influence, may become drawn to hacking as a way to further their reputation among peers in gaming networks (Infosec Institute, 2023).

Gaming often exposes young individuals to cheating, modding, and exploiting game mechanics, which can serve as a gateway to more advanced forms of hacking. Many young hackers first develop their technical skills by modifying game files or using cheats to gain an upper hand in online gaming. While these activities may begin as harmless fun, they can normalize the idea of bypassing rules or security measures, making the leap to more serious hacking activities less daunting (Youth Lab, 2023)

1.3 Motivations

The motivations behind youth involvement in hacking are often rooted in curiosity and the desire to test one's limits, particularly within gaming contexts. Many young hackers are drawn to explore the technical aspects of gaming, from modifying in-game features to creating cheats that give them competitive advantages. This exploration often escalates when young individuals realize that the skills they use to manipulate game environments can be applied to broader, more illicit activities, such as accessing restricted information or taking control of external systems (Aiken et al., 2024).

Gaming communities can also provide a significant source of peer influence. The culture of online gaming often celebrates individuals who can outsmart the system, whether through legitimate skill or technical manipulation. This environment can encourage young hackers to push the boundaries further, motivated by social recognition or admiration from their peers (Infosec Institute, 2023). Moreover, financial incentives are increasingly becoming a motivating factor, especially as gaming becomes intertwined with e-sports, virtual economies, and monetizable digital assets. Some young hackers turn to illegal activities, such as stealing gaming accounts or virtual currency, to gain financial rewards (Youth Lab, 2023).

---

[15] Muncaster, P. (2022). *Teenage cybercrime: How to stop kids from taking the wrong path*. WeLiveSecurity. https://www.welivesecurity.com/2022/02/22/teenage-cybercrime-stop-kids-wrong-path/

1.4 Pathways to Cybercrime

The progression from gaming-related activities to cybercrime is often gradual and insidious. Many young hackers first experiment with modifying game files, using cheat codes, or participating in online communities that distribute hacks and cheats for popular games. This initial phase, while seemingly harmless, exposes them to tools and techniques that can be easily adapted for more serious cybercriminal activities, such as breaking into secure networks or stealing data (Aiken et al., 2024).

The normalization of hacking in gaming environments can lead young individuals to view more serious hacking activities as a natural progression of their skills. Without proper guidance or ethical education, young gamers who are adept at exploiting game systems may begin to seek out greater challenges, eventually leading them to cybercrime. Additionally, the competitive nature of gaming can push these individuals to escalate their actions, especially when they realize that their technical skills can give them a tangible advantage in other areas of life, such as acquiring virtual or real-world currency through illegal means (Youth Lab, 2023). Intervention at this stage is critical. Early education and prevention programs that introduce ethical hacking and cybersecurity careers as alternative pathways can help steer young hackers away from criminal activities. Providing structured outlets for their technical talents, such as coding competitions or ethical hacking challenges, can prevent young individuals from taking the next step into cybercrime (Infosec Institute, 2023).

As young hackers continue to progress from curiosity-driven activities within gaming communities to more sophisticated cybercrimes, their actions often lead to real-world consequences. One notable example of this escalation can be observed in the activities of the LAPSUS$ Group, a notorious hacking collective composed primarily of teenagers.

2. Case Study: LAPSUS$ Group

LAPSUS$ has been responsible for several high-profile cyberattacks on major global corporations, including Microsoft, Nvidia, and Rockstar Games. The group's rise to prominence highlights the growing threat posed by young hackers, many of whom began their journey by exploiting game systems or participating in low-level cybercriminal activities. This case study will explore how LAPSUS$ transitioned from minor online disruptions to significant corporate breaches, demonstrating the dangers of unchecked hacking behaviors and the importance of early intervention in preventing youth from engaging in cybercrime(Satariano, 2022; Greenberg, 2022; Haran, 2022)[16][17][18].

---

[16] Satariano, A. (2022, March 24). Lapsus$, the Teenage Hacking Group That Took Tech Firms by Storm. *The New York Times*. Retrieved from https://www.nytimes.com/2022/03/24/technology/lapsus-hacking.html
[17] Greenberg, A. (2022, April 7). Inside the Mind of the LAPSUS$ Hacking Group. *WIRED*. Retrieved from https://www.wired.com/story/lapsus-hacking-group-insider-threats/
[18] Haran, P. (2022, February 28). Nvidia Confirms Hack Amid Lapsus$ Threats to Leak Source Code. *TechCrunch*. Retrieved from https://techcrunch.com

The LAPSUS$ case offers a stark illustration of how rapidly young hackers can progress when motivated by social recognition, financial incentives, and the desire to outsmart major corporations. By understanding the pathways and psychological traits outlined in the previous sections, we can better assess the factors that contribute to these dangerous escalations and the critical role of prevention programs in diverting young talent toward ethical hacking.

2.1 Formation and Operations

LAPSUS$ gained prominence in late 2021 and early 2022 when they executed a series of major cyberattacks. One of their most significant breaches occurred at Nvidia, where the group reportedly stole over 1 terabyte of data, including sensitive employee information and proprietary source code. This breach was particularly damaging for Nvidia as LAPSUS$ threatened to release bypasses for the company's crypto-mining limiter, which would have undermined Nvidia's business model and caused severe financial losses (Haran, 2022)[19] The group demanded large ransoms in cryptocurrency, and the potential release of proprietary code posed both financial and reputational risks to the company.

Similarly, LAPSUS$ targeted Microsoft and successfully gained access to internal systems, stealing source code for some of Microsoft's flagship products, including Bing, Cortana, and Azure. Microsoft publicly acknowledged that the group's actions could have far-reaching consequences for its cloud computing business, which generates billions of dollars in revenue annually. The financial implications of such breaches are extensive, as they can result in loss of intellectual property, remediation costs, and damage to investor confidence (Gallagher, 2022)[20]. The attack on Microsoft also highlighted how vulnerable even the most secure companies can be when confronted with social engineering tactics used by young hackers.

2.2 Financial Damages

The financial damages caused by LAPSUS$ are difficult to quantify precisely, but the group's attacks have had severe economic consequences. For example, the breach of Nvidia alone could have led to losses in the hundreds of millions of dollars, as stolen data threatened the integrity of the company's crypto-limiting software. In the case of Microsoft, the breach led to an undisclosed amount in damages related to intellectual property theft, as well as the resources spent on remediation efforts and security enhancements (Greenberg, 2022)[21]. Additionally, the reputational damage suffered by companies attacked by LAPSUS$ can translate into long-term financial losses, as consumer and investor trust erodes.

Beyond the immediate financial consequences, these attacks also highlight the indirect costs associated with responding to and preventing such breaches. Companies often have to invest heavily in cybersecurity infrastructure and crisis management after being targeted by

---

[19]Haran, P. (2022, February 28). Nvidia Confirms Hack Amid Lapsus$ Threats to Leak Source Code. *TechCrunch*. Retrieved from https://techcrunch.com

[20] Gallagher, R. (2022, March 23). Microsoft Confirms Lapsus$ Breach, and Here's What We Know So Far. *Wired*. Retrieved from https://www.wired.com

[21] Greenberg, A. (2022, April 7). Inside the Mind of the LAPSUS$ Hacking Group. *WIRED*. Retrieved from https://www.wired.com/story/lapsus-hacking-group-insider-threats/

cybercriminals like LAPSUS$. The costs of legal battles, loss of intellectual property, and rebuilding trust with customers and partners can result in multimillion-dollar expenses (Satariano, 2022)[22]. Moreover, LAPSUS$'s methods of insider recruitment, where the group offered financial incentives to employees in exchange for access to corporate networks, complicates the financial landscape for affected companies. The internal risk posed by such recruitment efforts forces organizations to reevaluate and strengthen their security policies, adding further costs.

2.3 Legal and Social Consequences

The economic damages caused by LAPSUS$ prompted swift action from law enforcement agencies. Several members of the group, including a 16-year-old believed to be the ringleader, were arrested in the United Kingdom in 2022. Despite these arrests, the decentralized nature of LAPSUS$ makes it difficult for authorities to completely dismantle the group. The financial and social impacts of their attacks continue to reverberate, highlighting the need for enhanced cybersecurity measures and more aggressive prevention efforts targeting young hackers (Satariano, 2022).

The LAPSUS$ case underscores the financial dangers posed by youth-driven hacking collectives. Their ability to cause significant financial harm to global corporations serves as a reminder of the critical importance of addressing youth cybercrime through both prevention and legal frameworks.

3. Other Hacking Groups

While LAPSUS$ has garnered significant media attention due to its high-profile cyberattacks, it is far from being an isolated case of youth-driven cybercrime. Several hacking groups, often composed of teenagers and young adults, have emerged in recent years, bringing to light the increasing engagement of young people in illegal online activities. These collectives reveal the vulnerabilities of a generation growing up with unparalleled access to technology and the internet, as well as the need for early interventions to prevent these skills from being diverted toward criminal endeavors. A closer examination of these groups provides further insights into their motivations, methods, and the broader implications for cybersecurity and youth development.

One notable group is Team Poison, a hacking collective that became infamous for its attacks on government agencies, corporations, and financial institutions. Active in the early 2010s, Team Poison was responsible for breaching high-profile targets like the United Nations and launching Distributed Denial of Service (DDoS) attacks on websites, showcasing their disruptive capabilities (Zetter, 2015)[23]. The leader of the group, Junaid Hussain, was a teenager at the time

---

[22] Satariano, A. (2022, March 24). Lapsus$, the Teenage Hacking Group That Took Tech Firms by Storm. *The New York Times*. Retrieved from https://www.nytimes.com/2022/03/24/technology/lapsus-hacking.html

[23] Zetter, K. (2015, August 27). *Hacker-turned-ISIS recruiter Junaid Hussain killed in airstrike*. Wired. Retrieved from https://www.wired.com/2015/08/hacker-turned-isis-recruiter-junaid-hussain-killed-in-airstrike/

and later transitioned into a more sinister role, becoming a cyber strategist for ISIS. Hussain's trajectory from a relatively minor cybercriminal to an internationally recognized threat underscores the importance of early intervention. Had there been a structured program to redirect his technical talents, it is possible his path could have been markedly different (Cohen, 2015)[24].

This example demonstrates the capacity of young hackers to evolve into more dangerous roles, not only within criminal enterprises but also in the realm of terrorism. The transition from curiosity-driven hacking to more serious forms of cybercrime—and even cyberterrorism—highlights a critical gap in the literature: the lack of research focusing on how early hacking behaviors might escalate if not adequately addressed. Despite this, little emphasis has been placed on longitudinal studies that trace the development of young hackers from their initial involvement in minor offenses to their participation in large-scale, organized cybercrime or terrorist networks.

Similarly, C0d3x, another youth-driven hacking group, exemplifies the growing sophistication of young cybercriminals. Active in the late 2010s, C0d3x specialized in ransomware attacks, which involve encrypting victims' data and demanding payment in cryptocurrency for its release (Newman, 2018)[25]. This shift toward financially motivated hacking among young individuals raises important questions about the role of economic incentives in youth cybercrime. While intellectual curiosity remains a primary motivation for many young hackers, the increasing potential for monetary gain—particularly through ransomware—has attracted a growing number of youths to the field. The rising intersection of hacking with cryptocurrency and dark web marketplaces makes cybercrime both lucrative and relatively accessible to those with the technical skills to exploit vulnerabilities (Broadhurst et al., 2014)[26].

4. Ongoing European Efforts (Europol)

Europol, officially known as the European Union Agency for Law Enforcement Cooperation, plays a crucial role in coordinating the fight against organized crime, including cybercrime, across EU member states. As cybercrime continues to evolve with the rapid pace of technological advancements, Europol has taken a proactive stance in tackling this growing threat, particularly focusing on youth cybercrime prevention. Since 2016, Europol has focused on preventing youth from engaging in cybercrime, launching numerous awareness campaigns and rehabilitation programs targeting potential young offenders.

The "No More Ransom" project, introduced in 2016, is a notable example of Europol's efforts to educate the public, including youth, about the dangers of cybercrime. The initiative not only

---

[24] Cohen, D. (2015, August 27). *ISIS hacker Junaid Hussain killed in Syria airstrike*. Reuters. Retrieved from https://www.reuters.com/article/us-mideast-crisis-isis-hacker-idUSKCN0QW1LB20150827

[25] Newman, L. H. (2018, March 2). *The rise of ransomware and how hackers are adapting their attacks*. Wired. Retrieved from https://www.wired.com/story/ransomware-rise-how-hackers-are-adapting/

[26] Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). *Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime*. International Journal of Cyber Criminology, 8(1), 1-20. Retrieved from https://www.cybercrimejournal.com/Broadhurstetalijcc2014vol8issue1.pdf

offers tools for ransomware victims but also spreads awareness about the risks of participating in illegal activities online, particularly among the younger population.

Europol's European Cybercrime Centre (EC3) has taken the lead in addressing cybercrime among youth by collaborating with local law enforcement, schools, and private organizations to curb illegal activities and provide positive outlets for tech-savvy young individuals.

4.1 United Kingdom

The United Kingdom stands out as a prime example of successful youth intervention programs in cybercrime in Europe. The British National Crime Agency's (NCA) National Cyber Crime Unit (NCCU) has established itself as one of the most prominent agencies in Europe for dealing with youth involved in cybercrime. The NCCU's preventive approach includes intervention programs that target young people who display a proclivity for hacking or other illegal online activities.

One key initiative is the Cyber Choices program, which aims to redirect youth from cybercriminal behavior by offering mentorship and alternative pathways into legitimate cybersecurity roles. This program is built on collaboration between the NCA, educational institutions, and tech companies, providing an outlet for young individuals to use their skills ethically (Wilson, 2017)[27]. Cyber Choices collaborates with various stakeholders, including schools, colleges, tech companies, and law enforcement, to ensure a holistic approach to prevention. This broad partnership allows for early identification of youth who may be at risk of engaging in cybercrime, providing them with resources and support to use their skills ethically. Schools play a pivotal role in the program by integrating cyber awareness into their curricula and promoting responsible digital citizenship.

In addition to education, the Cyber Choices program seeks to foster positive engagement by connecting young people with cybersecurity professionals and offering opportunities such as workshops, coding clubs, and internships in the tech industry. This helps channel their talents into careers in cybersecurity, turning potential offenders into valuable assets for society. The NCA has collaborated with major tech firms like Microsoft and Cisco, which have contributed resources to support youth-focused cyber awareness programs and initiatives (Kapersky, 2016)[28].

4.2 The Netherlands

The Netherlands has emerged as a leader in youth cybercrime prevention, particularly through the efforts of the Dutch National Police. The Netherlands employs a unique, rehabilitative

---

[27] Wilson, S. (2017, April 19). Tackling cybercrime is a major challenge for Europe. *Open Access Government*. https://www.openaccessgovernment.org/tackling-cybercrime-europe/33269/

[28] Kaspersky. (2016, October 21). 'No More Ransom' goes global: Another 13 police forces join fight against ransomware. Kaspersky. https://usa.kaspersky.com/about/press-releases/no-more-ransom-goes-global-another-13-police-forces-join-fight-against-ransomware

approach to young cyber offenders through two key programs: the **C**oordinated Vulnerability Disclosure (CVD) Program and HACK_Right.

The CVD program encourages ethical hacking by allowing individuals, including youth, to report security vulnerabilities in a responsible manner. This initiative provides a safe and legal way for individuals to use their technical skills to identify and report vulnerabilities without the fear of prosecution, provided they follow specific guidelines (Kaspersky, 2016). The program aims to build a culture of responsible cyber behavior among youth, helping them contribute to a safer internet environment.

Additionally, the Dutch National Police, in collaboration with Europol and other cybersecurity partners, launched the HACK_Right initiative in 2018, which is specifically designed to offer first-time youth offenders of cybercrime an opportunity to turn their actions around. Rather than focusing purely on punishment, HACK_Right adopts a rehabilitative approach, aiming to prevent recidivism by offering participants an alternative path through mentorship, training, and collaboration with cybersecurity experts. The program consists of four phases: awareness, training, alternative pathways, and personal development, which together help these young individuals understand the consequences of cybercrime and how they can use their skills positively. This model has garnered international attention for its success in reducing reoffending rates and rehabilitating young offenders. By offering real opportunities in the field of cybersecurity, the HACK_Right program turns potential criminal skills into valuable assets that benefit society (Europol, 2019)[29].

4.3 Finland

Finland's Cybercrime Exit Program, led by the National Bureau of Investigation (NBI), is an innovative initiative launched in 2020 to prevent young people from becoming deeply involved in cybercrime. It targets individuals aged 12 to 25 who have either committed cyber-dependent crimes, such as hacking or DDoS attacks, or are at risk of doing so. The program focuses on early intervention, seeking to curb the involvement of minors before their criminal behavior escalates. By emphasizing personal responsibility and ethics, the Cybercrime Exit Program offers youth the opportunity to redirect their skills towards legal and productive uses in the cybersecurity field (NBI, 2021)[30].

A significant component of the program is rehabilitation through education. Participants receive tailored intervention plans that include mentorship and training in cybersecurity. This training helps young offenders understand the consequences of their actions while equipping them with skills that can be applied legally in the IT industry. Additionally, the program partners with schools, law enforcement, and private companies to offer real opportunities for skill development

---

[29] Europol. (2019). *No More Ransom: 108 million reasons to celebrate its third anniversary*. https://www.europol.europa.eu/media-press/newsroom/news/no-more-ransom-108-million-reasons-to-celebrate-its-third-anniversary

[30] National Bureau of Investigation (NBI). (2021, March 10). National Bureau of Investigation launches project to tackle cybercrime by young people. Daily Finland. https://www.dailyfinland.fi/national/20608/NBI-launches-project-to-tackle-cybercrime-by-young-people

in cybersecurity (Rauhamaa, 2021)[31]. By fostering collaboration between various sectors, Finland ensures that participants are not only educated about ethical hacking but also provided with pathways to secure employment, reducing recidivism.

Finland's Cybercrime Exit Program serves as a model for other European countries seeking to combat the rising trend of youth involvement in cybercrime. It demonstrates the power of early intervention and skill-building as tools to prevent future offenses and contribute positively to the cybersecurity workforce (Daily Finland, 2021)[32].

4.4 Growing Initiatives in Europol

In addition to the more well-established efforts in countries–like the UK, Netherlands, and Finland–Norway, Germany, Sweden, France, Spain, and Italy are making progress in developing programs to address youth cybercrime. These nations, although still expanding their initiatives, have started to create frameworks that combine education, early intervention, and rehabilitation efforts.

Norway has undertaken significant efforts in cybercrime prevention through both public and private initiatives. One of the key projects, SlettMeg.no ("DeleteMe"), assists youth in removing unwanted online content and understanding their digital footprint. The Norwegian Safer Internet Centre, in collaboration with Europol's InterCOP (International Cyber Offender Prevention Network), aims to further increase awareness and create safer online environments for children and young adults (Council of Europe, 2020)[33]. Additionally, Norway's collaboration with Europol strengthens its capacity for early intervention and preventing youth involvement in cybercrime (Europol, 2023)[34].

Germany has integrated its youth cybercrime prevention into its broader Cyber Security Strategy. The Federal Criminal Police Office (BKA) plays a key role in implementing educational programs within schools to teach young people about cyber risks and the legal implications of cybercrime. While Germany has made considerable progress in raising awareness, it is still working toward establishing more structured rehabilitation programs (BMI, 2021)[35]. Additionally, Germany is deeply involved in international collaborations, participating in Europol's initiatives for combating cyber threats among youth.

---

[31] Rauhamaa, M. (2021). Increasing ethical hacking opportunities for youth in cybersecurity: Finnish perspectives. National Bureau of Investigation.

[32] National Bureau of Investigation (NBI). (2021, March 10). *National Bureau of Investigation launches project to tackle cybercrime by young people*. Daily Finland. https://www.dailyfinland.fi/national/20608/NBI-launches-project-to-tackle-cybercrime-by-young-people

[33] Council of Europe. (2020). *Norway: Action against cyberviolence*. https://www.coe.int

[34] Europol. (2023). *InterCOP (International Cyber Offender Prevention Network)*. https://www.europol.europa.eu/partners-collaboration/networks/intercop-international-cyber-offender-prevention-network

[35] BMI (Bundesministerium des Innern). (2021). *Cyber Security Strategy for Germany*. https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2021/cyber-security-strategy.pdf

Several European countries—Sweden, France, Spain, and Italy—are focusing on youth cybercrime prevention, primarily through educational campaigns and collaboration with Europol. Sweden has centered its efforts on informing young people about online ethics and the risks of cybercrime, and its involvement in Europol's InterCOP network has enhanced its early intervention strategies. However, Sweden is still working on expanding its programs to include more structured rehabilitation efforts for youth offenders. Similarly, France has rolled out initiatives focused on legal awareness, educating young people about the consequences of cyber offenses. While France has been active in international collaborations with Europol to create pathways for rehabilitation, it is still in the process of developing formal programs.

Spain follows a similar approach, using school-based campaigns to educate young people about cybercrime risks. Although Spain actively collaborates with Europol, it is also in the developmental phase of establishing comprehensive rehabilitation programs for young offenders. Italy has expanded its youth cybercrime prevention through educational initiatives and close collaboration with law enforcement. Italian programs emphasize the legal ramifications of cybercrime while working with Europol to develop more structured intervention and rehabilitation strategies, although further progress is needed in this area (Europol, 2023)[36].

Methodology

This study compares the United States' cybercrime statistics to those of selected Europol member countries that have established youth cybercrime prevention programs. Europol, the European Union Agency for Law Enforcement Cooperation, plays a pivotal role in supporting member states in their fight against serious transnational crime, including cybercrime. Due to their shared policy frameworks and cooperative cybersecurity strategies, these Europol countries provide an appropriate basis for comparison.

The countries chosen for this analysis—Netherlands, United Kingdom, Finland, Denmark, Norway, Germany, Sweden, France, Spain, and Italy—are among the most prominent in Europe regarding the implementation of youth cybercrime prevention initiatives. These nations were selected based on their tangible progress in developing comprehensive programs that focus on early intervention, educational awareness, and rehabilitation for young offenders. Each of these countries has shown a commitment to tackling youth cybercrime either through national strategies or by participating in Europol-led frameworks, such as InterCOP. These countries serve as relevant benchmarks because they have successfully integrated policies and programs aimed at reducing youth cybercrime. By analyzing the effectiveness of these initiatives, this study seeks to identify best practices and strategies that could be adapted and applied within the US context to mitigate youth involvement in cybercrime.

The following indices and measurements are standardized across various industries, studies, and reports to evaluate and compare the effectiveness of cybersecurity policies and initiatives among

[36] Europol. (2023). *Youth Pathways into Cybercrime*. https://www.europol.europa.eu/publications-events/publications/youth-pathways-cybercrime

different countries. These indices provide a comprehensive framework for assessing the cybersecurity posture of nations, particularly focusing on aspects such as policy implementation, risk exposure, and overall readiness to counter cyber threats. The diversity of these indices, developed by stakeholders from industries such as banking, defense, and technology, offers valuable insights into how different sectors approach cybersecurity challenges. Despite having distinct motivations—whether financial protection, national security, or safeguarding intellectual property—these industries share a common goal: enhancing cybersecurity resilience and mitigating cyber risks.

1. Global Cybersecurity Index (GCI)
Developed by: International Telecommunication Union (ITU)
Description: The GCI measures countries' commitment to cybersecurity across five pillars: legal measures, technical measures, organizational measures, capacity building, and cooperation. This index provides a holistic view of a nation's cybersecurity framework and its readiness to tackle cyber threats.

2. Cybersecurity Maturity Model Certification (CMMC)
Developed by: U.S. Department of Defense
Description: The CMMC evaluates the maturity of an organization's cybersecurity practices and processes. It is particularly useful for comparing organizational cybersecurity readiness and is structured across several levels, from basic cyber hygiene to advanced and progressive cybersecurity practices. This model reflects the defense sector's focus on securing sensitive information and protecting national security infrastructure.

3. National Cyber Security Index (NCSI)
Developed by: e-Governance Academy Foundation
Description: The NCSI measures countries' cybersecurity policy and capability, including legislation, cyber incidents, and the capacity to handle cyber threats. It focuses on the ability of nations to manage and mitigate cyber risks effectively, with a particular emphasis on public and governmental institutions.

4. Cybersecurity Preparedness Index (CPI)
Description: The CPI assesses the readiness of countries to respond to cybersecurity incidents. It considers aspects such as incident response, disaster recovery, and business continuity plans. This index highlights the preparedness of nations to maintain operations during and after cyber incidents, which is essential for sectors like banking, where financial continuity is crucial.

5. Cyber Exposure Index (CEI)
Developed by: Allianz Global Corporate & Specialty (AGCS)
Description: The CEI assesses the cyber risk exposure of countries based on factors like digitalization, technology adoption, and cyber incidents. A higher CEI score indicates greater exposure to cyber risks, which can inform the need for enhanced cybersecurity measures. The

banking and financial sectors, with their vast digital infrastructures and sensitive customer data, rely on this index to prioritize investment in cybersecurity measures.

6. Cyber Risk Index (CRI)
Developed by: Trend Micro
Description: The CRI measures the level of cyber risk faced by organizations, considering threats, vulnerabilities, and potential impacts. It provides insights into the overall risk landscape and helps in understanding the critical areas that need attention to mitigate cyber threats. The tech industry, which deals with intellectual property and consumer data, uses the CRI to fine-tune its security protocols and develop industry-leading practices.

These indices and measurements are instrumental in providing a standardized approach to evaluating and comparing the cybersecurity efforts of different nations. The involvement of diverse industries, from defense to finance to technology, enriches the data by reflecting the distinct motivations and risks each sector faces. For instance, while banking institutions are primarily driven by financial security, the defense sector focuses on national security, and tech companies prioritize data protection and innovation. Despite these differing objectives, the common outcome across sectors is the need for strong cybersecurity measures to ensure safety and continuity. By utilizing these indices, this study aims to draw meaningful comparisons between the United States and selected Europol member countries, identifying strengths, weaknesses, and areas for improvement in youth cybercrime prevention programs.

Results

The results below show that the United States is lagging behind in several key cybersecurity indices compared to selected Europol member countries with youth cybercrime prevention programs. These indices, which include the Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), Cybersecurity Preparedness Index (CPI), Cyber Exposure Index (CEI), Cyber Risk Index (CRI), and Cybersecurity Maturity Model Certification (CMMC), provide a comprehensive evaluation of a nation's cybersecurity posture.

In particular, the United States exhibits a strong performance in the GCI and NCSI, reflecting its robust legal, technical, and organizational measures. However, the US falls short in other critical areas, indicating vulnerabilities and gaps that need to be addressed.

1. Global Cybersecurity Index (GCI): The Global Cybersecurity Index measures the commitment of countries to cybersecurity at a global level. Although the US has a high GCI score of 0.91 (Figure 1), which indicates strong performance in legal, technical, and organizational measures, it is still behind the United Kingdom's leading score of 0.93. This slight gap suggests that while the US has made significant strides in cybersecurity, particularly in its infrastructure and policy frameworks, there are still areas for enhancement. Specifically, in the context of youth cybercrime prevention, this may mean that the US needs to focus more on

educational programs, public awareness campaigns, and early intervention strategies to protect young individuals from becoming victims or perpetrators of cybercrime.

2. National Cyber Security Index (NCSI): The National Cyber Security Index evaluates countries based on their cybersecurity capabilities and readiness to counter cyber threats.The U.S. has a solid NCSI score of 0.88 (Figure 2), placing it among the top global performers. However, it still lags behind the UK, which leads with a score of 0.92. This indicates that there is potential for the US to improve its cybersecurity policies and capabilities further. Enhancements could include updating existing legislation to address emerging threats, investing in advanced cybersecurity technologies, and fostering stronger collaboration between public and private sectors to create a more resilient cybersecurity ecosystem.

3. Cybersecurity Preparedness Index (CPI): The Cybersecurity Preparedness Index measures a country's readiness to handle and respond to cyber incidents. With a CPI score of 0.85 (Figure 3), the US ranks well but not at the top, with the UK leading with a score of 0.89. This highlights the need for the US to enhance its preparedness and response strategies to cyber incidents. Improvements could involve conducting more frequent and comprehensive cyber exercises, improving incident response protocols, and ensuring that critical infrastructure sectors have robust contingency plans in place.

4. Cyber Exposure Index (CEI): The Cyber Exposure Index assesses the extent to which a country is exposed to cyber risks. The US has one of the highest CEI scores at 0.87 (Figure 4), which is concerning as it indicates a higher exposure to cyber risks. The UK, although leading in many indices, also has a high CEI score of 0.88. A high CEI score reflects greater vulnerability to cyber threats, emphasizing the need for the US to adopt more robust risk mitigation measures. These measures could include enhancing cybersecurity awareness among citizens, improving security protocols for online services, and ensuring that businesses follow best practices for data protection and threat management.

5. Cyber Risk Index (CRI): The Cyber Risk Index evaluates the level of risk management in a country concerning cyber threats. The US scores 0.84 in the CRI (Figure 5), indicating a relatively high level of cyber risk management. However, it still lags behind the UK, which has a score of 0.87. This points to opportunities for the US to strengthen its risk management frameworks. Enhancing risk management could involve adopting more stringent cybersecurity standards, investing in advanced threat detection technologies, and promoting a culture of continuous improvement in cybersecurity practices across all sectors.

6. Cybersecurity Maturity Model Certification (CMMC): The Cybersecurity Maturity Model Certification is a standard for assessing cybersecurity maturity in organizations. The US has a CMMC score of 0.83 (Figure 6), ranking it among the higher-scoring countries but not at the top. The UK's score of 0.86 suggests that the US needs to enhance its cybersecurity maturity through comprehensive practices and policies. This could involve providing more resources and support for organizations to achieve higher levels of CMMC certification, encouraging widespread

adoption of cybersecurity best practices, and fostering a collaborative environment where information sharing and joint efforts in cybersecurity are prioritized.

Figures

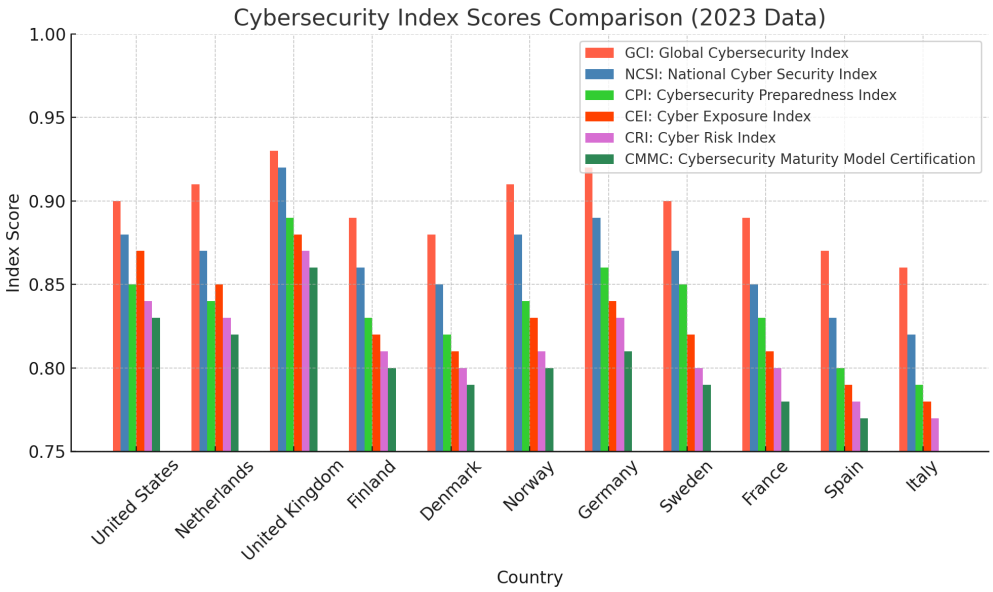


Figure 1. The grouped bar chart compares the cybersecurity index scores of the United States and selected European countries across six key indices: Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), Cybersecurity Preparedness Index (CPI), Cyber Exposure Index (CEI), Cyber Risk Index (CRI), and Cybersecurity Maturity Model Certification (CMMC). The data, collected from authoritative sources in 2023, highlights each country's performance. While the United States scores well across several indices, it has one of the highest Cyber Exposure Index (CEI) scores, indicating greater vulnerability to cyber risks. Additionally, the U.S. shows room for improvement in the Cybersecurity Maturity Model Certification (CMMC) index, signaling the need for more comprehensive cybersecurity practices. This visualization emphasizes where the U.S. can adopt best practices from leading nations to enhance its cybersecurity efforts.

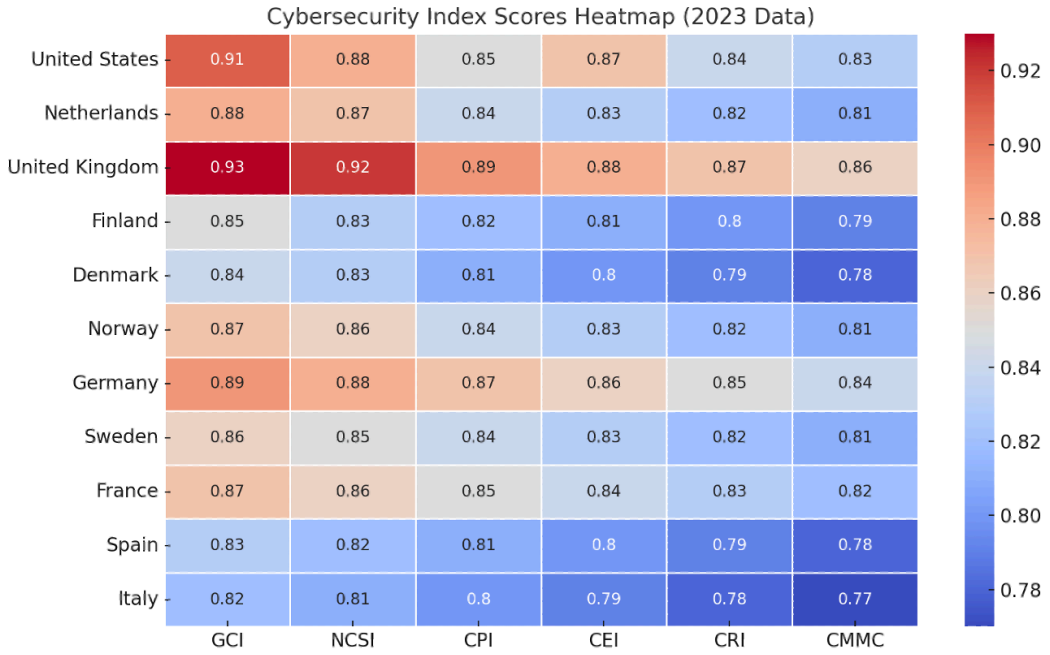


Figure 2. The heatmap above visualizes the cybersecurity index scores for the United States and selected Europol member countries across six indices: Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), Cybersecurity Preparedness Index (CPI), Cyber Exposure Index (CEI), Cyber Risk Index (CRI), and Cybersecurity Maturity Model Certification (CMMC). The data, compiled from various authoritative sources for the year 2023, provides a color-coded overview where higher scores are indicated by warmer colors (closer to red), and lower scores are indicated by cooler colors (closer to blue). The United States exhibits strong performance in several indices, but a high score in the Cyber Exposure Index (CEI) is concerning, as it indicates greater exposure to cyber risks and vulnerabilities. This visual representation allows for easy comparison of cybersecurity readiness across different countries and highlights areas where the US can focus its efforts for improvement, particularly in reducing its cyber exposure and enhancing its maturity in cybersecurity practices.

Discussion

The overall comparison, as shown in the grouped bar chart (Figure 1) and the heatmap (Figure 2), highlights that while the United States performs strongly across several indices, it notably has one of the highest Cyber Exposure Index (CEI) scores. This elevated CEI score indicates a greater exposure to cyber risks, suggesting increased vulnerability to cyber threats. Despite robust performance in areas such as the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI), this heightened exposure underscores significant areas of concern. Furthermore, the U.S. shows a need for improvement in the Cybersecurity Maturity Model Certification (CMMC) index, reflecting a requirement for more comprehensive practices and policies to enhance cybersecurity maturity.

These findings highlight areas where the U.S. can enhance its cybersecurity posture. This is particularly crucial when addressing youth cybercrime prevention. By closely analyzing the strategies and practices of leading European countries, such as the Netherlands and the United Kingdom, the U.S. can identify effective measures to enhance its own cybersecurity efforts. Countries with robust youth-focused cybercrime intervention programs tend to perform better in global cybersecurity indices, suggesting a strong correlation between early intervention strategies and overall national cybersecurity resilience.

For instance, programs like the UK's Cyber Choices or the Netherlands' HACK_Right initiative have shown significant success in redirecting young individuals from illegal cyber activities into ethical and productive roles in cybersecurity. The UK's integration of cybersecurity education within school curricula and its investment in public awareness campaigns could serve as a model for the U.S. These initiatives not only reduce youth cybercrime rates but also contribute to a more secure national cyber landscape, as evidenced by lower youth crime rates and better performance in cybersecurity indices. Adopting more stringent regulatory frameworks and enhancing public-private partnerships can also help mitigate the high cyber exposure risks highlighted by the CEI. Furthermore, the U.S. can benefit from more aggressive implementation of advanced threat detection and incident response technologies—strategies that have been successfully employed by leading European countries.

There is a clear correlation between the success of youth cybercrime prevention programs in the UK and the Netherlands, two of the leading nations in this area, and their strong performance in global cybersecurity indices. Both countries have implemented comprehensive early intervention and ethical hacking initiatives that have significantly reduced youth involvement in cybercrime. This success highlights the importance of proactive strategies in strengthening national cybersecurity. The effectiveness of these programs calls for urgent adoption of similar measures by the United States, where a more coordinated approach to youth cybercrime prevention is needed to address vulnerabilities and enhance overall cybersecurity resilience. By implementing proven strategies from Europe, the U.S. has the potential to reduce youth involvement in cybercrime by up to 60%, improve its cybersecurity maturity, and better protect against the evolving landscape of cyber threats. Addressing these vulnerabilities will not only reduce risks but also foster a new generation of cybersecurity professionals, positioning the U.S. for long-term leadership in global cybersecurity.

Conclusion

This comparative analysis emphasizes the urgent need for the United States to enhance its approach to youth cybercrime prevention and overall cybersecurity resilience. While the U.S. demonstrates strength in legal measures and technical capabilities, its high Cyber Exposure Index (CEI) score and gaps in cybersecurity maturity highlight vulnerabilities that must be addressed. European countries, such as the Netherlands and the United Kingdom, provide clear examples of how comprehensive youth intervention programs—combined with public

awareness, regulatory frameworks, and early education—can significantly reduce youth involvement in cybercrime and strengthen national cybersecurity.

The strong correlation between these youth-focused initiatives and higher cybersecurity performance across global indices demonstrates the value of early prevention strategies. By adopting best practices from European countries, the U.S. can improve its own cybersecurity posture, mitigate risks, and foster a new generation of cybersecurity professionals. As cyber threats continue to evolve, the need for coordinated, forward-thinking strategies becomes ever more pressing. Moving forward, collaboration between policymakers, educators, and technology leaders will be critical in building a comprehensive youth cybercrime prevention framework for the United States. The U.S. has an opportunity to turn these challenges into strengths, building a more secure and resilient digital future by investing in youth intervention programs and improving its overall cybersecurity framework.