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

Cynthia Tan

Faculty Mentor: Dr. James Patton Rogers, Executive Director, Brooks Tech Policy Institute, Cornell University
Supervisor: William McKeen, FBI Supervisory Special Agent, National Cyber-Forensics Training Alliance

Introduction

Cybercrime has become a significant global threat, with financial and security implications expected to escalate as the digital landscape continues to grow. By 2024, cyberattacks are projected to cost the global economy $9.5 trillion annually. A particularly concerning trend is the early engagement of youth in cybercrime, with many starting as early as their teenage years. This early involvement highlights the importance of developing effective prevention strategies targeted at young individuals.

While various countries have recognized the importance of youth-focused cybercrime prevention, the United States lags in implementing comprehensive early intervention programs. By contrast, countries in the European Union for Law Enforcement Cooperation, the law enforcement agency of the European Union, such as the United Kingdom, the Netherlands, and Finland have developed innovative approaches that divert youth from illegal cyber activities into ethical hacking and cybersecurity careers. These strategies include educational interventions, mentorship programs, and ethical hacking initiatives that have proven effective in reducing youth participation in cybercrime.

The central question this study seeks to answer is: How can the United States improve its youth-focused cybercrime prevention efforts by adopting early intervention and educational strategies from European nations with established cybercrime reduction programs?

This study compares the United States' efforts to those of leading European nations in the field of youth cybercrime prevention. By analyzing global cybersecurity indices such as the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI), this study aims to identify best practices and strategies that can be adapted to the U.S. context. The findings suggest that while the U.S. performs well in areas such as legal and technical frameworks, it has significant gaps in youth-focused cybercrime prevention, particularly in educational outreach and early intervention.

Methodology

This study compares the United States' cybercrime statistics with selected European countries in Europol—**the United Kingdom, the Netherlands, Finland, Denmark, Norway, Germany, Sweden, France, Spain, and Italy**. These countries were chosen due to their established youth cybercrime prevention programs and comprehensive early intervention, education, and rehabilitation initiatives. Europol's coordinated frameworks make these countries suitable for comparison.

The following global indices, each developed by reputable organizations with strong expertise in cybersecurity and risk management, were used to evaluate and compare the effectiveness of cybersecurity policies among these nations:

1. Global Cybersecurity Index (GCI):
Developed by the International Telecommunication Union (ITU), this index assesses countries' commitment to cybersecurity through legal, technical, and organizational measures.

2. Cybersecurity Maturity Model Certification (CMMC):
Developed by the U.S. Department of Defense, the CMMC evaluates the maturity of an organization's cybersecurity practices across several levels, from basic hygiene to advanced practices.

3. National Cyber Security Index (NCSI):
Created by the e-Governance Academy Foundation, this index measures a country's ability to manage and mitigate cyber risks, focusing on public and governmental institutions.

4. Cybersecurity Preparedness Index (CPI):
This index assesses the readiness of countries to respond to cyber incidents, focusing on incident response and disaster recovery capabilities.

5. Cyber Exposure Index (CEI):
Developed by Allianz, the CEI measures countries' exposure to cyber risks based on technology adoption and digitalization.

6.Cyber Risk Index (CRI):
Created by Trend Micro, the CRI evaluates a country's overall level of cyber risk based on threats and vulnerabilities, helping to prioritize risk mitigation strategies.

These indices provide a framework for comparing the U.S. to European countries, helping identify best practices that could be adapted to improve youth cybercrime prevention in the U.S.

Results

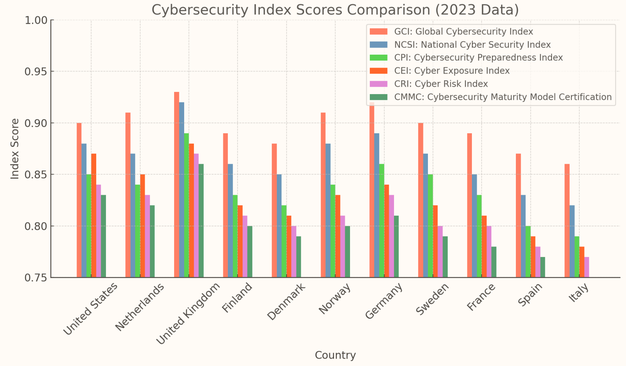

Figure 1. The grouped bar chart compares the cybersecurity index scores of the United States and selected European countries—Netherlands, United Kingdom, Finland, Denmark, Norway, Germany, Sweden, France, Spain, and Italy—across six indices: Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), Cybersecurity Preparedness Index (CPI), Cyber Exposure Index (CEI), Cyber Risk Index (CRI), and Cybersecurity Maturity Model Certification (CMMC). The bar chart clearly shows each country's performance in 2023 for these indices, with taller bars representing higher scores. For example, the United States demonstrates strong scores in the GCI (0.91) and NCSI (0.88), but its high score in the CEI (0.87) signals greater exposure to cyber risks, indicating vulnerability. The United Kingdom leads in both the GCI (0.93) and NCSI (0.92), showcasing its strong legal and organizational cybersecurity measures. The Netherlands performs consistently with a GCI of 0.88 and NCSI of 0.87, reflecting a solid cybersecurity framework, though its CEI score of 0.83 suggests slightly better risk management compared to the U.S. Countries like Italy, on the other hand, show lower scores, with a GCI of 0.82 and CMMC of 0.77, revealing areas for improvement in cybersecurity maturity. This bar chart provides a direct visual comparison, highlighting the specific strengths and weaknesses of each country's cybersecurity posture. It reveals opportunities where the U.S. can improve its cybersecurity practices by learning from higher-performing nations like the U.K., particularly in enhancing cybersecurity maturity and reducing exposure to risks.

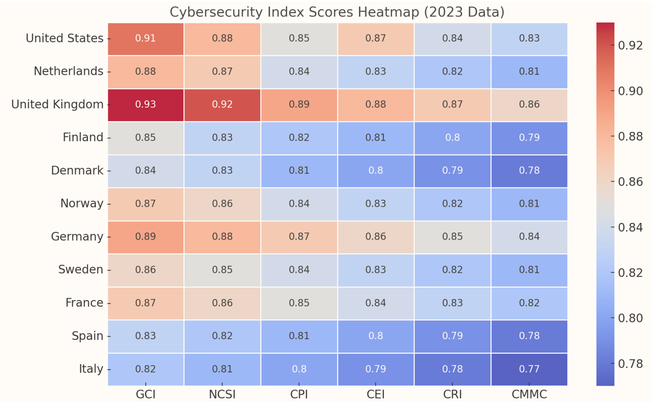

Figure 2. The heatmap above visualizes the cybersecurity index scores for the United States and selected Europol member countries across six indices: Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), Cybersecurity Preparedness Index (CPI), Cyber Exposure Index (CEI), Cyber Risk 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). For example, the United States scores 0.91 in the GCI, 0.88 in the NCSI, and 0.87 in the CEI, with the latter being a high score indicating greater exposure to cyber risks. The UK shows a leading GCI score of 0.93 and NCSI score of 0.92, demonstrating strong cybersecurity measures across multiple indices. Meanwhile, countries like Italy score 0.82 in the GCI and 0.77 in the CMMC, suggesting areas for improvement in cybersecurity maturity and readiness. This visual representation allows for easy comparison of cybersecurity readiness across different countries and highlights areas where the U.S. can focus its efforts for improvement, particularly in reducing its cyber exposure and enhancing its maturity in cybersecurity practices.

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 significant vulnerabilities that must be addressed. The U.S. lags behind European countries like the Netherlands and the United Kingdom, which have implemented effective youth cybercrime prevention programs and demonstrated lower rates of youth involvement in cybercrime.

Findings from this study show that countries with comprehensive youth-focused programs tend to perform better across cybersecurity indices. For example, the Netherlands and the UK's early intervention initiatives—such as ethical hacking programs and educational efforts—have led to a reduction in youth cybercrime by up to 60%. These efforts have not only improved their cybersecurity rankings but have also nurtured a new generation of cybersecurity professionals.

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 future 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.

References

1.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
2.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
3.BMI (Bundesministerium des Innern). (2021). Cyber Security Strategy for Germany. https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2021/cyber-security-strategy.pdf
4.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
5.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
6.Council of Europe. (2020). Norway: Action against cyberviolence. https//www.coe.int
7.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
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.Dedovic, Y. (2020). Cybercrime: Internet erodes teenage impulse controls. ScienceDaily. https://www.sciencedaily.com/releases/2020/01/200121112915.htm
10.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
11.Europol. (2023). InterCOP (International Cyber Offender Prevention Network). https://www.europol.europa.eu/partners-collaboration/networks/intercop-international-cyber-offender-prevention-network
12.Europol. (2023). Youth Pathways into Cybercrime. https://www.europol.europa.eu/publications-events/publications/youth-pathways-cybercrime
13.FBI. (2023). Internet Crime Report 2023. Internet Crime Complaint Center. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
14.Gallagher, R. (2022, March 23). Microsoft Confirms Lapsus$ Breach, and Here's What We Know So Far. Wired. Retrieved from https://www.wired.com/story/okta-hack-microsoft-bing-code-leak/
15.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/
16.Gregory, J. (2022, August 30). Why teens become cyber criminals. Security Intelligence. Retrieved from https://securityintelligence.com/articles/why-teens-become-cyber-criminals/
17.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
18.Morgan, S. (2023, October 25). Cybercrime to cost the world $9.5 trillion annually in 2024. Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/#:~=A%20breakdown%20of%20global%20cybercrime,%24182.5%20billion%20USD%20a%20week
19.Muncaster, P. (2022). Teenage cybercrime: How to stop kids from taking the wrong path. WeLiveSecurity. https://www.welivesecurity.com/2022/02/22/teenage-cybercrime-stop-kids-wrong-path/
20.National Bureau of Investigation (NBI). (2021, March 10). National Bureau of Investigation launches project to tackle cybercrime by young people. Daily Finland. https://www.dailyfinland.fi/national/20608/NBI-launches-project-to-tackle-cybercrime-by-young-people
21.Noordegraaf, J. E., & Kranenbarg, M. (2023, October 11). Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. Criminology, 61(1), 121-145. doi:10.1111/1745-9133.12650
22.Rauhamaa, M. (2021). Increasing ethical hacking opportunities for youth in cybersecurity: Finnish perspectives. National Bureau of Investigation.
23.Satariano, A. (2022, March 24). Lapsus$, 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
24.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
25.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
26.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
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.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