Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 31

11-18-2024

Integrating Humanities into Cybersecurity Education: Enhancing Ethical, Historical, and Sociopolitical Understanding in Technical Training

Joseph Frusci
The College of Staten Island, CUNY, joseph.frusci@csi.cuny.edu

Integrating Humanities into Cybersecurity Education: Enhancing Ethical, Historical, and Sociopolitical Understanding in Technical Training

Abstract

The increasing complexity of cybersecurity challenges necessitates a holistic educational approach that integrates both technical skills and humanistic perspectives. This article examines the importance of infusing humanities disciplines such as history, ethics, political science, sociology, law, and anthropology—into cybersecurity education. Through a pilot course developed for Staten Island Technical High School, aligned with the New York State K-12 Computer Science and Digital Fluency Standards, students were introduced to an interdisciplinary curriculum that combined technical cybersecurity training with historical analysis, ethical reasoning, and sociopolitical context. The results of pre- and post-course assessments demonstrated significant improvements in critical thinking, ethical decision-making, and the ability to evaluate cybersecurity issues from a broader societal perspective. This article discusses how an interdisciplinary approach not only enhances students' technical competencies but also prepares them to address the ethical and societal dimensions of cybersecurity, making a case for incorporating humanities into the cybersecurity education curriculum at both secondary and post-secondary levels.

Keywords

Cybersecurity Education, Humanities Integration, Ethical Reasoning, Sociopolitical Analysis, STEM Curriculum, Critical Thinking, Cybersecurity Ethics, High School Cybersecurity, Global Cybersecurity Policies

Cover Page Footnote

This research was conducted as part of a pilot course developed for Staten Island Technical High School, aligned with the New York State K-12 Computer Science and Digital Fluency Standards. The author would like to acknowledge the contributions of the faculty and staff at Staten Island Technical High School for their support in implementing the course. Special thanks to the students who participated in the course, whose feedback and engagement were integral to this study's success.

Integrating Humanities into Cybersecurity Education: Enhancing Ethical, Historical, and Sociopolitical Understanding in Technical Training

Joseph Frusci, Ed.D.
The College of Staten Island, CUNY
Staten Island, NY
joseph.frusci@csi.cuny.edu
0000-0002-6033-1237

Abstract— **The increasing complexity of cybersecurity challenges necessitates a holistic educational approach that integrates both technical skills and humanistic perspectives. This article examines the importance of infusing humanities disciplines such as history, ethics, political science, sociology, law, and anthropology, into cybersecurity education. Through a pilot course developed for 12th-grade students, aligned with the New York State K-12 Computer Science and Digital Fluency Standards, students were introduced to an interdisciplinary curriculum that combined technical cybersecurity training with historical analysis, ethical reasoning, and sociopolitical context. The results of pre- and post-course assessments demonstrated significant improvements in critical thinking, ethical decision-making, and the ability to evaluate cybersecurity issues from a broader societal perspective. This article discusses how an interdisciplinary approach not only enhances students' technical competencies but also prepares them to address the ethical and societal dimensions of cybersecurity, making a case for incorporating humanities into the cybersecurity education curriculum at both secondary and post-secondary levels.**

Keywords— Cybersecurity Education, Humanities Integration, Ethical Reasoning, Sociopolitical Analysis, STEM Curriculum, Critical Thinking, Cybersecurity Ethics, High School Cybersecurity, Global Cybersecurity Policies Introduction

I. Introduction

As cybersecurity threats evolve and become more complex, so must the education systems designed to prepare the next generation of cybersecurity professionals. Traditional cybersecurity education has focused heavily on technical skills such as cryptography, network security, and software development, often at the expense of a broader, interdisciplinary approach. However, as technological advancements permeate all facets of society, cybersecurity professionals are increasingly required to make ethical decisions, understand the societal implications of their work, and navigate the legal and political ramifications of cyberattacks. To meet these challenges, the integration of humanities disciplines—such as history, ethics, law, political science, sociology, and anthropology into cybersecurity education is not only beneficial but essential.

Interdisciplinary learning plays a critical role in equipping students with the skills necessary to address not just the technical aspects of cybersecurity, but also the ethical, legal, and societal dimensions. As Ess (2009) argues, the ethical implications of digital technologies are too significant to be sidelined in education, and a grounding in ethics can help students navigate complex moral dilemmas related to privacy, surveillance, and digital rights. Similarly, Brey (2017) highlights that understanding the ethical frameworks surrounding emerging technologies allows cybersecurity professionals to anticipate the broader impacts of their decisions on individuals and society. Without these humanistic considerations, cybersecurity professionals may lack the necessary tools to engage with the ethical challenges posed by issues such as data breaches, algorithmic bias, and surveillance capitalism.

Beyond ethics, disciplines like history and political science provide critical insights into the broader sociopolitical context in which cybersecurity operates. Singer and Friedman (2014) emphasize that understanding the historical evolution of cyberwarfare and state-sponsored cyberattacks is essential for navigating today's geopolitical landscape. Case studies such as the Stuxnet and WannaCry attacks illustrate how political and historical contexts shape both the strategies of attackers and the responses of governments and private entities (Sanger, 2018). Thus, integrating historical analysis into cybersecurity education allows students to develop a deeper understanding of how past events inform current and future challenges.

Moreover, sociology and anthropology offer crucial insights into human behavior and the cultural implications of cybersecurity. As technology becomes increasingly enmeshed in daily life, understanding how different cultures and societies interact with technology becomes vital. Turkle

(2011) points out that technology shapes not only our personal relationships but also our broader social structures. By integrating sociological and anthropological perspectives into cybersecurity education, students gain a more nuanced understanding of how human behavior influences cybersecurity threats, and vice versa.

In response to this growing need for interdisciplinary approaches, I developed a pilot cybersecurity course for 12th-grade students that incorporated humanities disciplines, aligned with the *New York State K-12 Computer Science and Digital Fluency Standards*. This course was designed to foster critical thinking, ethical reasoning, and an awareness of the societal and historical dimensions of cybersecurity. The pilot course included historical case studies of significant cybersecurity events, ethical debates on data privacy and surveillance, and discussions on the role of law and policy in regulating technology. Through these interdisciplinary lenses, students were encouraged to think beyond technical solutions and consider the broader implications of their actions in a complex and interconnected world.

This article will examine the outcomes of this pilot course, with a particular focus on how integrating the humanities into cybersecurity education can enhance students' critical thinking, ethical decision-making, and interdisciplinary awareness. By bridging the gap between technical expertise and humanistic understanding, this approach prepares students not only to solve cybersecurity problems but also to navigate the ethical and societal dimensions of the field. This interdisciplinary framework, as supported by scholars such as Floridi and Taddeo (2016), is essential for educating well-rounded cybersecurity professionals equipped to meet the demands of an increasingly interconnected and ethically fraught digital world.

II. LITERATURE REVIEW

As the complexity and scope of cybersecurity threats increase, the need for cybersecurity professionals to possess more than just technical skills has become widely recognized. Integrating humanities disciplines, such as ethics, sociology, history, and political science, into cybersecurity education has been identified as an important step toward creating well-rounded professionals capable of addressing not only the technical challenges of the field but also the broader societal, ethical, and geopolitical implications. Recent research has focused on the value of interdisciplinary education in cybersecurity, where both technical and humanistic knowledge are crucial to addressing modern cybersecurity issues (Payne & Hadzhidimova, 2020).

Cybersecurity challenges today involve more than preventing and responding to attacks. They include understanding global policies, ethical dilemmas, legal frameworks, and the societal impact of digital threats. This section reviews the theoretical grounding and key studies that support the incorporation of humanities into cybersecurity education and how this interdisciplinary approach provides a more comprehensive framework for understanding the complexities of the field.

A. Theoretical Grounding and Interdisciplinary Education

In recent years, the importance of integrating humanities disciplines—such as ethics, sociology, and political science—into cybersecurity education has gained widespread recognition. As cybersecurity issues grow more complex, scholars argue that technical knowledge alone is insufficient to address the multifaceted challenges of the field. This has led to a broader push for interdisciplinary approaches that equip students with both technical proficiency and a nuanced understanding of the societal, ethical, and geopolitical dimensions of cybersecurity (Burley, Eisenberg, & Goodman, 2014).

B. Ethical Frameworks in Cybersecurity

The integration of cyber ethics into education has become increasingly important, given the ethical dilemmas faced by cybersecurity professionals. Ethical frameworks, such as utilitarianism and deontological ethics, help students navigate challenges involving data privacy, surveillance, and the balance between security and civil liberties. Scholars like Floridi and Taddeo (2016) emphasize that cybersecurity professionals must not only secure systems but also consider the ethical implications of their actions, such as the societal impact of surveillance or the trade-offs between privacy and national security.

Similarly, Nissenbaum (2010) explores how privacy is shaped by broader social and political contexts. Her work highlights the importance of understanding privacy not just as a technical issue but as a social construct that reflects societal values. By incorporating ethical reasoning into cybersecurity education, students are better prepared to address real-world dilemmas, such as government surveillance or corporate data breaches, with a strong moral foundation.

C. Sociological Perspectives on Cybersecurity

Sociology also plays a critical role in understanding cybersecurity's broader societal impact. Scholars such as Deibert (2013) have noted that cybersecurity is inherently sociopolitical, shaped by power dynamics between governments, corporations, and individuals. Cyberattacks do not occur in a vacuum; they are influenced by social structures, political interests, and cultural norms. For example, state-sponsored cyberattacks, like the Stuxnet incident, reflect broader geopolitical struggles and raise ethical questions about the use of digital weapons in international conflicts.

By incorporating sociological analysis into cybersecurity education, students are better equipped to understand how cyberattacks can affect different communities and regions in varied ways. Additionally, the study of social engineering—the manipulation of individuals to gain unauthorized access to

systems—underscores the human element in cybersecurity. Teaching students about the sociological factors that contribute to vulnerabilities, such as trust and authority, helps them develop strategies to mitigate human-related security risks.

D. Political Science and Global Governance

The role of political science in cybersecurity education is vital, as cybersecurity is deeply entwined with international relations and global governance. As Deibert (2013) and Singer and Friedman (2014) note, cybersecurity has become a central issue in global politics, with nation-states vying for control over information, infrastructure, and digital resources. Political science provides students with the tools to understand how global cybersecurity policies, such as the General Data Protection Regulation (GDPR) in Europe or China's Great Firewall, shape the digital landscape and affect cybersecurity practices.

By analyzing case studies of international cyberattacks and data breaches, students can develop a deeper understanding of how political forces influence cybersecurity policies. This knowledge is crucial for addressing the global nature of cybersecurity threats, which often transcend national borders. Political science frameworks also help students evaluate the legal and regulatory challenges associated with cybersecurity, providing them with a broader perspective on issues like international data privacy laws, cyberwarfare, and global cybercrime.

E. Integrating Interdisciplinary Approaches in Cybersecurity Education

The intersection of ethics, sociology, and political science with cybersecurity education enhances students' ability to navigate the ethical, social, and political complexities of the field. As Payne and Hadzhidimova (2020) argue, non-technical knowledge is essential for developing well-rounded cybersecurity professionals who can think critically about the broader implications of their work. Interdisciplinary education encourages students to approach cybersecurity challenges not just as technical problems but as issues that have real-world consequences for individuals, societies, and governments.

By combining these disciplines, the Humanities in Cybersecurity course equips students to analyze cyberattacks and defenses from multiple perspectives, enabling them to become cybersecurity professionals who are not only technically skilled but also socially and ethically aware. This holistic approach is increasingly necessary in a world where cybersecurity issues are complex, interconnected, and global in scope.

F. Case Studies and Interdisciplinary Applications

Beyond theoretical frameworks, case studies provide concrete examples of how humanities-based approaches to cybersecurity education can be applied. Sanger (2018), for example, discusses the Sony Pictures hack and how understanding the geopolitical context helped cybersecurity experts navigate the incident's fallout. By incorporating these case studies into the classroom, educators can demonstrate the real-world relevance of ethical and political frameworks. Research has also shown that integrating historical case studies into technical curricula enhances students' ability to think critically about past cybersecurity incidents and apply those lessons to current challenges (Pfleeger & Pfleeger, 2006). For instance, analyzing the Stuxnet attack not only deepens students' understanding of the technical vulnerabilities exploited but also helps them reflect on the geopolitical implications of cyber warfare.

G. Interdisciplinary Cybersecurity Education in Practice

Recent efforts in cybersecurity education have further underscored the need for interdisciplinary approaches. Burley et al. (2014) argues for the professionalization of cybersecurity education, emphasizing that technical expertise must be supplemented by ethical decision-making and an understanding of the social and political environment. Similarly, Payne and Hadzhidimova (2020) assert that cybersecurity curricula should incorporate more non-technical content to help students develop the critical thinking and problem-solving skills needed to address modern cybersecurity challenges.

III. METHODS

The research for the Humanities in Cybersecurity course utilized a mixed methods study to assess the effectiveness of integrating humanities disciplines—such as ethics, history, sociology, and political science—into a traditionally technical cybersecurity curriculum. The mixed methods approach combined quantitative and qualitative data collection techniques to provide a comprehensive evaluation of student learning outcomes. This section outlines the course design, data collection procedures, and analysis methods used in the study.

A. Course Design Overview

The Humanities in Cybersecurity course was structured as an interdisciplinary program aimed at providing high school seniors with an integrated understanding of cybersecurity, combining technical skills with ethical, historical, and sociopolitical perspectives. Aligned with the *New York State K-12 Computer Science and Digital Fluency Standards*, the course aimed to develop students' critical thinking, ethical reasoning, and ability to understand the broader societal implications of cybersecurity.

The course consisted of 16 units, each of which focused on a specific aspect of cybersecurity (e.g., network security, data privacy) and incorporated relevant humanities content. Each unit included practical case studies, reflective writing, discussions, and collaborative projects that allowed students to apply both technical and humanistic knowledge.

B. Mixed Methods Data Collection

1) Quantitative Data Collection

Quantitative data was gathered through pre- and post-exams, rubric-based assessments, and surveys. These tools measured students' growth in technical knowledge, ethical reasoning, historical understanding, and sociopolitical awareness.

a. Pre- and Post-Exams: Students completed exams at the beginning and end of the course. The exams consisted of multiple-choice, short-answer, and Likert scale questions designed to assess their knowledge across technical, ethical, historical, and sociopolitical domains. The pre-exam established a baseline understanding of cybersecurity concepts, while the post-exam measured students' progress at the end of the course.

1. Technical Knowledge: Multiple-choice questions focused on core cybersecurity concepts such as encryption, multi-factor authentication, and network security.

2. Ethical Reasoning: Likert scale questions assessed students' ability to apply ethical frameworks to real-world cybersecurity scenarios, such as privacy issues and government surveillance.

3. Historical and Sociopolitical Awareness: Short-answer questions asked students to analyze key historical cybersecurity events (e.g., Stuxnet, Morris Worm) and assess their sociopolitical implications.

b. Rubric-Based Assignments: Students' final projects and case study analyses were graded using rubrics that evaluated their ability to synthesize technical, ethical, historical, and sociopolitical perspectives. Each assignment was scored across categories such as content mastery, ethical reasoning, historical analysis, and sociopolitical context.

c. Surveys: Students completed surveys at the end of the course to measure their perceived growth in understanding the ethical, historical, and sociopolitical aspects of cybersecurity. Surveys included both close-ended Likert scale questions and open-ended questions for deeper reflection.

2) Qualitative Data Collection

Qualitative data was collected through reflection papers, open-ended survey responses, and semi-structured interviews. This data provided insights into students' experiences with the course and their perceptions of how the interdisciplinary approach influenced their learning.

a. Reflection Papers: Each unit included a reflective writing assignment in which students were asked to critically engage with the ethical, historical, or sociopolitical content of the unit. These papers allowed students to articulate how the case studies and theoretical frameworks discussed in class influenced their understanding of cybersecurity issues.

b. Open-Ended Survey Responses: At the end of the course, surveys included open-ended questions that asked students to describe specific aspects of the course that impacted their learning. Responses were analyzed thematically to identify common themes, such as the value of ethical decision-making and the importance of historical context in understanding cybersecurity incidents.

c. Semi-Structured Interviews: A subset of students participated in post-course interviews designed to explore their experiences in greater depth. Interview questions focused on how students' understanding of cybersecurity evolved, particularly in relation to the ethical, historical, and sociopolitical dimensions. The interviews were recorded, transcribed, and analyzed for recurring themes.

C. Data Analysis

Quantitative data from the pre- and post-exams and rubric-based assessments were analyzed using descriptive statistics to measure changes in students' performance. The mean scores, standard deviations, and percentage improvements for each category (e.g., technical knowledge, ethical reasoning, historical context) were calculated to quantify growth.

1. Exam Scores: Improvements in pre- and post-exam scores were analyzed to determine growth in specific areas of knowledge. For example, scores on ethical reasoning questions were compared to identify the extent of students' growth in applying ethical theories to cybersecurity dilemmas.

2. Rubric Scores: Final project and assignment scores were analyzed to assess students' ability to integrate interdisciplinary knowledge into practical cybersecurity applications. The rubric scores allowed for a comparison of students' technical and non-technical growth throughout the course.

Qualitative data from reflection papers, open-ended survey responses, and interviews were analyzed using thematic analysis. This process involved coding student responses to

identify key themes related to ethical reasoning, historical understanding, and sociopolitical awareness.

1. Reflection Papers: Common themes across students' reflections were identified, such as increased ethical awareness, the ability to contextualize cybersecurity within historical events, and the recognition of global sociopolitical dynamics.
2. Open-Ended Responses and Interviews: Interview transcripts and open-ended survey responses were coded to uncover deeper insights into students' experiences. Themes such as the importance of ethics in decision-making, the relevance of historical case studies, and the global nature of cybersecurity emerged as central to students' interdisciplinary learning.

D. Triangulation of Data

To ensure a comprehensive understanding of students' learning outcomes, data from both the quantitative and qualitative assessments were triangulated. By comparing exam results with reflection papers and interviews, the study provided both numerical evidence of growth and deeper qualitative insights into how and why this growth occurred. For instance, the quantitative improvement in ethical reasoning was supported by students' qualitative reflections on applying ethical frameworks to real-world cybersecurity scenarios.

IV. Results

A. Quantitative Results: Pre- and Post-Exam Comparisons

The pre- and post-exam data revealed significant growth across key areas of the course, particularly in students' understanding of ethical reasoning, historical context, and interdisciplinary analysis. The exams assessed knowledge in four main categories: technical knowledge, ethical reasoning, historical context, and sociopolitical analysis.

1. Technical Knowledge: Students' understanding of core technical cybersecurity concepts improved by 20%, as measured by multiple-choice and short-answer questions on encryption, network security, and multi-factor authentication (MFA).
2. Ethical Reasoning: Growth in ethical reasoning was particularly strong, with a 37.5% improvement in students' ability to apply ethical frameworks to real-world cybersecurity scenarios. Pre-exam results indicated that students were initially unfamiliar with ethical theories such as utilitarianism and deontological ethics, but by the end of the course, students demonstrated a much stronger grasp of these frameworks.
3. Historical Context: There was a notable 18% increase in students' ability to analyze cybersecurity incidents within their historical and political contexts. Pre-exam responses tended to focus solely on technical aspects, whereas post-exam answers incorporated the historical evolution of cyberattacks, including examples like the Stuxnet and Morris Worm attacks.
    a. Sociopolitical Analysis: The greatest improvement was seen in students' ability to evaluate cybersecurity issues through a sociopolitical lens, with a 46% increase. This growth reflects a deeper understanding of the global and cultural implications of cyber policies, as well as the role of government and law in regulating cybersecurity practices.

B. Technical Knowledge Growth

There was a notable 20% improvement in students' understanding of core technical cybersecurity concepts, such as encryption, network security, and multi-factor authentication. On the pre-exam, students struggled with questions that required deeper technical knowledge, particularly when explaining security practices like multi-factor authentication (MFA) and the role

1. Pre-Exam Example: Many students answered the following technical question incorrectly:
    a. *"What is the primary function of a firewall?"*
        i. Pre-exam accuracy: 55%
    b. In contrast, by the post-exam, 90% of students could correctly identify the role of firewalls, showing strong technical knowledge growth.

C. Ethical Reasoning Group

Ethical reasoning showed one of the most significant improvements, with a 37.5% growth in students' ability to apply ethical frameworks to real-world cybersecurity scenarios. On the pre-exam, many students demonstrated limited understanding of ethical theories, often defaulting to simplistic answers when confronted with ethical dilemmas, such as government surveillance or privacy concerns.

1. Pre-Exam Example:
    a. *"To what extent is government surveillance justified in the interest of national security?"*
        1. Pre-exam Likert scale average: 3.2/5 (indicating moderate uncertainty).
2. Post-exam responses revealed a more nuanced understanding:
        1. Post-exam Likert scale average: 4.4/5, indicating a substantial shift

toward more informed ethical judgments.

Students' reflection papers and post-exam essays demonstrated their ability to draw from ethical frameworks such as utilitarianism, deontology, and virtue ethics. For example, one student wrote:

"Initially, I thought the Snowden leaks were simply a matter of right or wrong, but after analyzing the situation through deontology, I see how ethical decisions are rarely black and white. We must balance personal privacy with the protection of society, and that's where ethics comes into play."

This finding is consistent with the classroom discussions and case studies, such as the examination of Edward Snowden's NSA leaks, which provided students with real-world examples of ethical conflict in cybersecurity. This also explains the significant 37.5% growth observed in the ethical reasoning scores.

D. Historical Context Growth

Students' understanding of the historical context surrounding major cybersecurity events improved by 18%, as indicated by their ability to analyze incidents such as the Stuxnet attack and the Morris Worm through a historical lens. On the pre-exam, students often focused narrowly on technical aspects, such as malware or coding errors, without recognizing the geopolitical or social implications of these events.

1. Pre-Exam Example: In a question about the Stuxnet attack, students were asked to describe the event's broader implications. The average score on this question was 70%, with most students failing to acknowledge the attack's geopolitical ramifications.
2. Post-exam responses, however, incorporated a much deeper historical understanding:
    a. Post-exam score: 88%

    One student wrote:
    "Stuxnet wasn't just about disrupting Iran's nuclear program—it was a political weapon that revealed how cyberwarfare could destabilize international relations. Learning this helped me understand the historical weight behind modern cyberattacks."

This improvement reflects the effectiveness of incorporating historical case studies and discussions into the course. The use of case studies like Stuxnet not only helped students understand the evolution of cybersecurity practices but also contextualized modern cyber threats within broader historical, political, and cultural narratives.

E. Sociopolitical Analysis Growth

The largest increase (46%) was observed in students' ability to evaluate cybersecurity through a sociopolitical lens, reflecting a more nuanced understanding of the intersection between cybersecurity and societal, cultural, and governmental factors.

1. Pre-Exam Example: Students were asked to discuss the impact of GDPR (General Data Protection Regulation) on global privacy practices. The pre-exam average score was 2.8/5, with many students providing only surface-level descriptions of the law's technical aspects.
2. Post-exam responses showed significant growth, with an average score of 4.1/5. Students were able to discuss GDPR's broader implications, including its influence on corporate behavior, international relations, and individual privacy rights.

    a. One student commented:
    "GDPR has transformed how companies handle data, but it also raises questions about how much control governments should have over the internet. This made me think about how privacy laws reflect a society's values and priorities."

The significant 46% growth in sociopolitical understanding can be attributed to units focusing on global cybersecurity practices, such as China's Great Firewall, which offered students a glimpse into how cultural and governmental factors shape internet use and cybersecurity policies.

F. Qualitative Results: Thematic Analysis of Reflection Papers and Interviews

The qualitative data from reflection papers and interviews provides deeper insight into the quantitative growth observed in the pre- and post-exams. Thematic analysis identified several key areas where students demonstrated deeper thinking and interdisciplinary understanding.

1. Development of Ethical Reasoning:
    As highlighted in the quantitative data, ethical reasoning was an area of significant growth. Many students' reflections expressed how the course helped them move beyond simplistic ethical judgments, allowing them to engage more critically with complex cybersecurity dilemmas.
    a. Pre-Course Reflection Example:
    "I think cybersecurity should focus only on preventing attacks. I don't see how ethics is really involved—what matters is keeping systems safe."
    b. Post-Course Reflection Example:
    "Now I see that every decision in cybersecurity has ethical implications, whether it's balancing privacy rights or deciding how much access governments should have to personal data. Learning

about the Snowden case and using ethical frameworks helped me understand these complexities."

This growth in ethical reasoning aligns with the quantitative results, showing a 37.5% increase in students' ability to apply ethical theories in cybersecurity scenarios.

G. Integration of Historical Perspectives:

Students frequently referenced how the historical case studies broadened their understanding of cybersecurity beyond technical considerations. Several reflections emphasized how learning about past cyberattacks like Morris Worm and Stuxnet helped them see the evolution of cybersecurity as part of broader historical and political developments.

1. Interview Excerpt:
   "Before, I thought cybersecurity was just about stopping hackers. But after learning about the history of these attacks, like Morris Worm, I realized how much technology and politics are connected. Cyberattacks can change the course of history just like traditional wars."

These reflections provide a qualitative explanation for the 18% increase in students' historical understanding, as seen in the post-exam results.

H. Increased Sociopolitical Awareness

Sociopolitical awareness emerged as one of the most transformative areas of growth, with many students expressing a newfound understanding of how cybersecurity practices are shaped by cultural and governmental factors. This is particularly evident in reflections on the GDPR and China's Great Firewall.

1. Student Reflection Example:
   "Learning about China's internet control made me think about how different countries approach cybersecurity. It's not just about technology, it's about how governments control information and people. This has changed the way I think about global cybersecurity issues."

This increased sociopolitical awareness aligns with the 46% growth observed in the quantitative data and demonstrates how the course's interdisciplinary approach deepened students' understanding of the global implications of cybersecurity policies.

I. Rubric Based Assessment

The final project, which required students to integrate technical, ethical, historical, and sociopolitical perspectives in analyzing a real-world cybersecurity incident, further illustrates the overall growth demonstrated by the quantitative and qualitative data.

1. Ethical Analysis: The 35% growth in ethical analysis reflects the course's strong focus on ethical reasoning, particularly through case studies like the NSA leaks and Stuxnet. Many students were able to apply multiple ethical frameworks to analyze real-world cybersecurity dilemmas.
2. Sociopolitical Perspective: The 40% improvement in sociopolitical perspectives demonstrates the students' growing ability to think critically about how cultural, political, and legal factors shape cybersecurity practices.

J. Synthesis of Quantitative and Qualitative Findings

The integration of quantitative and qualitative data provides a robust and multidimensional understanding of students' growth. The quantitative improvements in ethical reasoning, historical analysis, and sociopolitical awareness are strongly supported by qualitative insights that show how students' thinking evolved. As the course progressed, students not only gained technical knowledge but also developed a deeper, more interdisciplinary understanding of cybersecurity, recognizing its ethical, historical, and societal complexities. This holistic growth highlights the success of integrating humanities into cybersecurity education, preparing students to navigate the multifaceted challenges of the field with a more critical and ethically informed perspective.

K. Figures and Tables

Table 1

Category	Pre-Exam Average Score	Post-Exam Average Score	Growth (%)
Technical Knowledge	65%	85%	20%
Ethical Reasoning	3.2/5	4.4/5	37.5%
Historical Context	70%	88%	18%
Sociopolitical Analysis	2.8/5	4.1/5	46%

Table 1:Quantitative Results: Pre- and Post-Exam Comparisons

Table 2

Rubric Category	Pre-Project Score	Post-Project Score	Growth (%)
Technical Knowledge	16/25	22/25	20%
Ethical Analysis	17/25	23/25	35%
Historical Context	14/25	21/25	28%
Sociopolitical Perspective	15/25	22/25	40%

Table 2: Rubric-Based Assessment of Final Projects

V. Discussion

The results of this study illustrate significant growth in students' interdisciplinary understanding of cybersecurity, particularly through the integration of the humanities. By combining technical knowledge with historical, ethical, and sociopolitical perspectives, the Humanities in Cybersecurity course fostered deeper critical thinking and problem-solving skills. This Discussion section will interpret these findings in the context of the course's methodology and broader educational research, while also addressing the challenges and implications for future cybersecurity education.

A. Interpretation of Key Findings

1. Growth in Ethical Reasoning and Decision-Making
One of the most notable outcomes of this course was the substantial improvement in students' ability to apply ethical reasoning to cybersecurity challenges. The 37.5% increase in ethical reasoning scores, as shown by the post-exam results, highlights the success of integrating ethics into cybersecurity education. Pre-course understanding of ethics was limited, with students initially seeing cybersecurity as purely technical. However, after studying case studies such as Edward Snowden's NSA leaks and applying ethical frameworks like utilitarianism and deontology, students were better equipped to analyze complex ethical dilemmas.

   The qualitative data from reflection papers reinforced this growth, with students expressing a newfound appreciation for the ethical dimensions of cybersecurity. As one student noted, *"I didn't realize how important ethics were in cybersecurity until I had to apply these theories to real-world cases. It's not just about stopping attacks—it's about making ethical choices that affect people's lives."*

   These results align with existing literature on interdisciplinary cybersecurity education, which emphasizes the need for students to develop strong ethical decision-making skills to address the moral dilemmas inherent in cybersecurity (Floridi & Taddeo, 2016; Ess, 2009). By contextualizing cybersecurity issues within ethical frameworks, the course equipped students to navigate the ethical trade-offs that arise in real-world cybersecurity scenarios, from data privacy to government surveillance.

2. Historical Contextualization of Cybersecurity
The inclusion of historical case studies in the course curriculum led to an 18% improvement in students' ability to place cybersecurity incidents within their broader historical and geopolitical contexts. This growth was particularly evident in the post-exam responses to questions about significant cyberattacks like Stuxnet and Morris Worm, where students demonstrated an understanding of how these events shaped modern cybersecurity practices.

   The integration of history allowed students to move beyond a purely technical focus and appreciate the long-term societal and political impacts of cyberattacks. One student's reflection, *"I didn't realize how much history affects the way we approach cybersecurity today,"* underscores the importance of understanding the evolution of cybersecurity threats and defenses. The historical context helped students see that cyberattacks are not isolated incidents but part of a larger narrative involving technological, political, and cultural forces.

   This finding is consistent with research by Singer and Friedman (2014) and Schneier (2015), which highlights the importance of teaching students about the historical evolution of cybersecurity to provide context for modern challenges. As cyberwarfare and state-sponsored attacks become more prevalent, understanding the historical precedents for these actions is critical for preparing future cybersecurity professionals.

3. Sociopolitical Awareness and Global Perspectives
The most significant growth was observed in students' sociopolitical understanding of cybersecurity, with a 46% improvement in the post-exam results. This growth reflects students' increased ability to analyze cybersecurity issues through a global and cultural lens, as demonstrated in their engagement with case studies such as China's Great Firewall and the General Data Protection Regulation (GDPR).

   Before the course, many students approached cybersecurity primarily from a technical or individualistic perspective, focusing on how to secure data or prevent attacks. However, by the end of the course, students were able to critically evaluate how different governments and cultures shape cybersecurity policies and practices. One student's reflection captures this shift: *"Studying how China controls the internet through the Great Firewall made me realize that cybersecurity is not just about technology—it's about power, control, and cultural values."*

   This growth supports the argument made by Deibert (2013) and Payne and Hadzhidimova (2020) that cybersecurity education must address the global political and cultural contexts in which cybersecurity operates. As cyberattacks increasingly cross borders, understanding the diverse legal, social, and political landscapes in which cybersecurity exists is essential for preparing professionals who can navigate these complexities.

B. *The Role of Interdisciplinary Education in Cybersecurity*

The success of the Humanities in Cybersecurity course provides strong evidence for the value of interdisciplinary approaches in cybersecurity education. Traditional cybersecurity curricula often prioritize technical skills, with little emphasis on the ethical, historical, or sociopolitical aspects of cybersecurity. However, this study demonstrates that integrating humanities disciplines into cybersecurity education not only improves students' technical knowledge but also deepens their critical thinking and problem-solving abilities.

The qualitative and quantitative results indicate that students who engaged with the course's interdisciplinary content developed a more nuanced understanding of cybersecurity, one that goes beyond technical proficiency to include ethical decision-making, historical awareness, and sociopolitical analysis. This finding aligns with research by Burley, Eisenberg, and Goodman (2014), who argue that cybersecurity professionalization requires both technical and non-technical knowledge.

By incorporating humanities subjects, the course provided students with the tools to think more broadly about cybersecurity and its impact on society. This holistic approach to cybersecurity education is crucial for developing well-rounded professionals who can address not only technical challenges but also the ethical and societal dimensions of cybersecurity.

C. *Challenges and Limitations*

While the results of this study are promising, the implementation of an interdisciplinary approach to cybersecurity education did present certain challenges.

1. *Student Resistance to Humanities in Cybersecurity*

Some students initially resisted the integration of humanities disciplines, expressing discomfort with the ethical and philosophical discussions that were outside their technical comfort zones. In early reflection papers, a few students questioned the relevance of studying ethics, history, or political science in a cybersecurity course, stating that they preferred to focus on technical skills.

However, as the course progressed, this resistance diminished. The qualitative data showed that by the end of the course, most students appreciated the interdisciplinary approach and recognized the value of humanities in shaping their understanding of cybersecurity. This shift is reflective of a broader challenge in cybersecurity education, where students and educators alike may prioritize technical skills over non-technical knowledge (Payne & Hadzhidimova, 2020). Addressing this challenge requires careful curriculum design and the incorporation of case studies and real-world applications that make the connections between humanities and cybersecurity more tangible.

2. *Time Constraints and Curriculum Overload*

Another challenge was the need to balance technical content with the humanities components within a limited time frame. The breadth of topics covered in the course—ranging from technical concepts like MFA and network security to ethical theories and historical case studies—required careful pacing to ensure that students had enough time to engage with both the technical and humanistic aspects of the course.

Some students expressed feeling overwhelmed by the variety of topics covered, particularly in units that demanded deep reflection on complex ethical or sociopolitical issues. While the interdisciplinary approach enriched their understanding, it also posed a challenge in terms of time management and depth of coverage. Future iterations of the course could address this by streamlining the curriculum or offering more flexible timelines for assignments and projects.

D. *Implications for Future Cybersecurity Education*

The findings from this study have important implications for the future of cybersecurity education. As cybersecurity threats continue to evolve in complexity, the need for professionals who can navigate not only the technical challenges but also the ethical, legal, and social dimensions of cybersecurity will become increasingly critical.

The integration of humanities disciplines into cybersecurity education offers a pathway to developing more well-rounded professionals who are equipped to address these multidimensional challenges. The Humanities in Cybersecurity course serves as a model for how interdisciplinary education can enhance critical thinking, ethical reasoning, and global awareness in cybersecurity students.

Future cybersecurity curricula should build on this model by continuing to incorporate ethics, history, sociology, and political science into technical training. This holistic approach will better prepare students for the real-world complexities of cybersecurity, where technical decisions are always influenced by ethical, legal, and societal considerations.

E. *Broader Applicability: Preparing Students for Higher Education and International Contexts*

The Humanities in Cybersecurity course equips high school students with a combination of technical skills and interdisciplinary knowledge, preparing them not only for immediate challenges in cybersecurity but also for further study in higher education and professional settings. The course's unique integration of humanities disciplines—such as ethics, history, sociology, and political science—ensures that

students are able to approach cybersecurity from multiple perspectives, providing them with a solid foundation as they transition into more technically demanding college-level programs. Moreover, this interdisciplinary approach is adaptable to various international educational contexts, allowing it to address the global nature of cybersecurity threats.

1. *Preparing Students for Higher Education*

As students progress from high school to college or university, they will encounter increasingly complex technical content, including cryptography, advanced network security, and cyber defense mechanisms. While these topics demand rigorous technical proficiency, the Humanities in Cybersecurity course prepares students for this transition by cultivating critical thinking and ethical reasoning skills alongside their technical training. By learning to analyze cybersecurity issues through both technical and non-technical lenses, students are better equipped to address the multifaceted challenges they will encounter in higher education.

For instance, students who have engaged with ethical frameworks like utilitarianism and deontological ethics will be more adept at navigating the moral dilemmas they may face in college-level cybersecurity courses. Similarly, students who have explored the sociopolitical dimensions of cybersecurity, such as the impacts of GDPR or the legal frameworks governing cybersecurity in the U.S., will be better prepared to engage with the legal and regulatory complexities that are increasingly central to the field. By bridging the gap between high school education and the technical demands of higher education, the course ensures that students can not only master the technical aspects of cybersecurity but also consider the broader ethical and societal implications of their work.

Additionally, the course's focus on case studies, such as the Stuxnet attack and Edward Snowden's NSA leaks, provides students with a real-world context for understanding the intersection between technology and ethics. These examples allow students to apply theoretical knowledge to practical scenarios, enhancing their ability to think critically and make informed decisions in a college or university setting. As they continue their studies, students will benefit from the interdisciplinary grounding they received in high school, which enables them to approach technical challenges with a more holistic understanding of their societal impact.

2. *Broader Applicability to Higher Education*

In addition to preparing students for higher education, the Humanities in Cybersecurity course's interdisciplinary framework can be adapted to meet the needs of college-level programs and international educational systems. In higher education, where the focus often shifts toward advanced technical training, incorporating the course's interdisciplinary approach can help bridge the gap between technical proficiency and the broader ethical, legal, and societal considerations of cybersecurity. By integrating ethics, history, and political science into the curriculum, universities can ensure that their students are well-rounded professionals who can address the complex ethical dilemmas and global challenges associated with cybersecurity.

For example, at the university level, students could engage in interdisciplinary capstone projects where they analyze real-world cybersecurity incidents and propose solutions that incorporate both technical expertise and ethical reasoning. These projects would allow students to apply the critical thinking skills they developed in high school to more advanced technical challenges, ensuring that they are prepared to handle the complexities of professional cybersecurity work. Moreover, universities could expand upon the ethical and legal frameworks introduced in the high school course, allowing students to explore issues such as GDPR compliance, international data privacy laws, and the legal implications of cyberattacks in greater depth.

The course is also well-suited for adaptation in international contexts, where different cultural, legal, and political factors shape how cybersecurity is taught and practiced. In regions like the European Union, where the General Data Protection Regulation (GDPR) emphasizes privacy and data security, the course could focus on privacy rights and data governance. In contrast, countries like China, with its Great Firewall and emphasis on state control of the internet, present a different set of challenges and opportunities for cybersecurity professionals (Deibert, 2013). By adapting the course to address these regional differences, educators can help students understand how cybersecurity is influenced by local laws, regulations, and cultural norms.

Furthermore, the course's focus on ethical reasoning and global governance makes it particularly valuable in regions where digital infrastructure is still developing. In countries that are building their cybersecurity capabilities, such as those in Africa or Southeast Asia, the course could provide a comprehensive introduction to both the technical and ethical aspects of cybersecurity. This interdisciplinary approach would not only prepare students to work within their own countries but also equip them to engage with international cybersecurity challenges, fostering global collaboration and awareness (Singer & Friedman, 2014).

By comparing different approaches to cybersecurity governance, such as the GDPR in the European Union and U.S. cybersecurity frameworks like the NIST Cybersecurity Framework, the course helps students develop a nuanced understanding of the international landscape of cybersecurity. This global perspective is

essential for professionals who will need to navigate the transnational nature of cyber threats, collaborate with international teams, and address the ethical and legal implications of working in a globally connected environment.

The Humanities in Cybersecurity course not only prepares students for success in higher education but also serves as a flexible model that can be adapted to meet the needs of students in various educational and international settings. By integrating technical skills with ethical reasoning and sociopolitical analysis, the course ensures that students are well-equipped to address the complex challenges of modern cybersecurity. Whether in high school, college, or across borders, the interdisciplinary approach fosters professionals who can tackle cybersecurity issues from both a technical and a humanistic perspective, making them valuable assets in an increasingly digital and interconnected world.

VI. Conclusion

The Humanities in Cybersecurity course, with its interdisciplinary approach, demonstrated the value of integrating humanities disciplines—such as ethics, history, sociology, and political science—into cybersecurity education. By combining technical training with the critical thinking skills developed through the humanities, the course equipped students to approach cybersecurity challenges with a more comprehensive, ethically informed, and globally aware mindset. This foundation not only prepares students for the complexities of real-world cybersecurity but also supports their transition into more technically demanding higher education programs, where they will further deepen their technical expertise while retaining a broader perspective.

A. Key Findings

Quantitative results showed significant improvement across several key areas. Students exhibited a 20% increase in technical knowledge, demonstrating a solid grasp of core cybersecurity concepts such as encryption, network security, and multi-factor authentication. However, the most substantial growth occurred in the domains of ethical reasoning (37.5%) and sociopolitical analysis (46%), reflecting the course's emphasis on interdisciplinary thinking. These findings suggest that students who were initially unfamiliar with ethical frameworks and the broader implications of cybersecurity were able to develop sophisticated perspectives on the societal and global impacts of cybersecurity incidents.

Qualitative data from reflection papers, surveys, and interviews further supported these findings. Students moved beyond seeing cybersecurity as merely a technical discipline, recognizing that real-world cybersecurity issues often involve complex ethical dilemmas and geopolitical considerations. Their reflections indicated a growing ability to apply ethical theories to analyze government surveillance, data privacy, and the long-term effects of cyberattacks on global security and culture.

B. Implications for Cybersecurity Education

The success of the Humanities in Cybersecurity course highlights the importance of a holistic approach to cybersecurity education. As cybersecurity threats evolve, the professionals who address them must be prepared to navigate not only the technical dimensions of the field but also the ethical, historical, legal, and sociopolitical complexities. Integrating humanities into cybersecurity curricula fosters well-rounded professionals who are capable of understanding the broader consequences of their actions and making decisions that take into account the needs of society.

Importantly, this interdisciplinary approach provides a strong foundation for students as they transition into higher education. While technical proficiency will be deepened in college-level cybersecurity programs, the ethical and critical thinking skills developed in this course will allow students to engage with more advanced technical challenges in a thoughtful and globally conscious manner. This ensures that they are not only prepared for the technical rigors of higher education but also equipped to approach cybersecurity problems from a multifaceted perspective.

C. Recommendations for Future Curriculum Design

Building on the results of this study, future cybersecurity curricula should continue to incorporate humanities-based education. Key recommendations for designing such curricula include:

1. Ethics Integration: Regularly integrate ethical frameworks and case studies into technical coursework to encourage students to consider the moral dimensions of their work.
2. Historical Case Studies: Use historical cyberattacks to contextualize modern cybersecurity challenges, helping students understand how past events inform current practices and policies.
3. Global Perspectives: Include lessons on international cybersecurity policies and cultural differences in data protection and internet governance, ensuring students are aware of the global implications of cybersecurity.
4. Capstone Projects: Offer interdisciplinary capstone projects where students analyze real-world cybersecurity incidents, applying technical, ethical, and sociopolitical knowledge to propose comprehensive solutions.

D. *Limitations and Future Research*

While this study demonstrated significant growth in students' technical knowledge, ethical reasoning, and sociopolitical analysis, several limitations should be considered. First, the study was conducted with a relatively small sample size and in a single educational setting, limiting the generalizability of the results. As such, the findings may not reflect the broader applicability of the course across diverse student populations or different educational institutions. Additionally, time constraints within the course structure made it challenging to delve deeply into certain complex topics, particularly those involving sociopolitical and ethical debates.

Moreover, while the study showed percentage improvements in students' knowledge and understanding, formal statistical tests, such as t-tests or ANOVA, were not conducted to determine the statistical significance of the differences between pre- and post-course results. Although the observed improvements in ethical reasoning (37.5%) and sociopolitical analysis (46%) are promising, future research could benefit from incorporating these tests to validate the significance of the observed growth. Using statistical tests would allow for a more rigorous assessment of whether the improvements are not only substantial but also statistically significant.

Future research could address these limitations by incorporating longitudinal studies that follow students beyond the completion of the course. Tracking students over several years—through their higher education experiences and early career stages—would provide a deeper understanding of how interdisciplinary cybersecurity education influences their ability to navigate real-world ethical, technical, and global challenges. Longitudinal data would also help assess the lasting impact of the course on students' professional success in the field of cybersecurity.

Additionally, future research should aim to replicate this study in a variety of educational contexts, including schools with different focuses (e.g., non-STEM institutions) and more diverse student populations. Conducting similar studies across different geographic and international settings would help validate the effectiveness of the interdisciplinary approach in cybersecurity education. Multiple case studies could further explore how the integration of humanities in cybersecurity education functions in countries with differing legal and regulatory frameworks, such as those governed by the General Data Protection Regulation (GDPR) in Europe or more restrictive internet governance models, like China's Great Firewall.

By expanding the scope of the research to include both longitudinal studies and case studies—and by incorporating formal statistical analyses—future efforts can provide a more comprehensive understanding of how humanities-infused cybersecurity education prepares students for the technical and ethical challenges of the digital age.

E. *Final Thoughts*

The increasing complexity of cybersecurity threats demands a new kind of professional—one who not only possesses technical skills but also understands the ethical, historical, and sociopolitical contexts in which cybersecurity operates. The Humanities in Cybersecurity course provides a model for how interdisciplinary education can prepare students to meet these challenges with the depth of understanding and critical thinking necessary for the modern cybersecurity landscape. As the field continues to evolve, the integration of humanities into cybersecurity education will be essential for developing professionals who can address the full spectrum of challenges posed by our increasingly digital world.

Furthermore, this interdisciplinary foundation offers an important steppingstone for students as they transition into higher education, where their advanced technical training will be strengthened by the ethical, historical, and global perspectives they have gained. By incorporating both technical and humanistic knowledge, future cybersecurity professionals will be better equipped to navigate the complex dilemmas and global challenges that are intrinsic to the digital era. As cybersecurity continues to transcend borders and involves sociopolitical considerations, the holistic approach demonstrated in this course ensures that students are prepared to think critically and act responsibly in an interconnected world.

VII. Acknowledgment

This work was made possible by the computer science and cybersecurity students at Staten Island Technical High School of the New York City Department of Education

VIII. References

[1] Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM*, 57(2), 24-27.

[2] Conklin, A. W., Cline, R. E., & Roosa, T. (2014). Re-engineering cybersecurity education in the US: An analysis of the critical issues. *Proceedings of the 2014 47th Hawaii International Conference on System Sciences*, 2006-2015.

[3] Deibert, R. J. (2013). Black Code: Surveillance, Privacy, and the Dark Side of the Internet. McClelland & Stewart.

[4] Ess, C. (2009). *Digital Media Ethics*. Polity Press.

[5] Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083), 20160111. https://doi.org/10.1098/rsta.2016.0111

[6] Kerr, O. S. (2004). The Fourth Amendment and new technologies: Constitutional myths and the case for caution. *Michigan Law Review*, 102(5), 801-888.

[7] Levy, S. (2010). Hackers: Heroes of the Computer Revolution. O'Reilly Media.

[8] Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

[9] Payne, B., & Hadzhidimova, L. (2020). Interdisciplinary cybersecurity education and the case for non-technical knowledge. *Journal of The Colloquium for Information System Security Education*, 7(2), 29-40.

[10] Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in Computing* (4th ed.). Prentice Hall.

[11] Roggema, R., Vermeulen, P. A., & Verwaart, T. (2019). Philosophy of technology in cyber education: On the role of the humanities in cyber educational practice. *Proceedings of the 2019 IEEE Global Engineering Education Conference (EDUCON)*, 1288-1292.

[12] Sanger, D. E. (2018). The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown Publishing.

[13] Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.

[14] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

[15] Taddeo, M., & Floridi, L. (2016). The ethics of information warfare: Cyber conflicts as the new 'normal'. *Ethics and Information Technology*, 18(2), 75-87. https://doi.org/10.1007/s10676-016-9399-6

[16] Turkle, S. (2011). Alone Together: Why We Expect More from Technology and Less from Each Other. Basic Books.