SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 03 No. 02 (2026), pp. 182-191
Research Article
doi: https://doi.org/10.70710/sitj.v3i2.104

Human Security Threat Analysis in the Cambridge Analytica Case Based on the UNDP 1994 Framework

Muhamad Umar Nugroho[1,a,*], Vina Selvia[1,b], Ardhian Dwi Saputra[1,c]

[1]Cryptographic Hardware Engineering Study Program, Department of Cryptography, Politeknik Siber dan Sandi Negara, Bogor, Indonesia
[a]muhamad.umar@student.poltekssn.ac.id; [b]vina.selvia@student.poltekssn.ac.id;
[c]ardhian.dwi@student.poltekssn.ac.id
*Corresponding author

Article Info
Received: 30-May-2026
Revised: 15-June-2026
Accepted: 30-June-2026

Keywords
Cambridge Analytica; Community Security; Digital Psychological Manipulation; Human Security; Micro-targeting; Personal Security; Political Security; Psychographic Profiling

Abstract
The rapid growth of digital technologies and social media platforms has created new challenges related to privacy, data protection, and information manipulation. One of the most prominent examples is the Cambridge Analytica scandal, in which personal data from millions of Facebook users were collected and utilized for psychographic profiling and political micro-targeting. This study aims to analyze the Cambridge Analytica case using the Human Security framework introduced by the United Nations Development Programme (UNDP) in the Human Development Report 1994. A qualitative case study approach was employed, utilizing literature review and document analysis from academic publications, official reports, investigative journalism, and policy documents related to Human Security, digital manipulation, and data exploitation. The findings indicate that the Cambridge Analytica scandal represents a contemporary Human Security threat in the digital era. The case primarily affected three dimensions of Human Security: political security, personal security, and community security. Political security was threatened through voter manipulation and interference in democratic processes; personal security was compromised through privacy violations and unauthorized data exploitation; while community security was weakened through the creation of echo chambers and increasing social polarization. The study also highlights that human vulnerabilities, including limited digital literacy, excessive trust in digital platforms, and susceptibility to psychological manipulation, played a significant role in enabling data exploitation. The findings suggest that strengthening digital literacy, improving data protection regulations, enhancing platform accountability, and promoting ethical digital governance are essential for safeguarding Human Security in the contemporary digital environment.

1. Introduction

The rapid development of digital technology and social media platforms has transformed the way people communicate, access information, and participate in political processes (Kim & Ellison, 2022). Platforms such as Facebook, Twitter, and Instagram have become important channels for public discourse, political campaigns, and information dissemination (Congge et al., 2023). While these technologies provide significant benefits for communication and democratic participation, they also create new challenges related to privacy, data protection, and information manipulation (Lorenz-Spreen et al., 2022).

In the digital era, personal data has become a valuable resource that can be collected, analyzed, and utilized for various purposes. Advances in Big Data analytics, artificial intelligence, and algorithmic

targeting have enabled organizations to understand individual behavior, preferences, and psychological characteristics with unprecedented accuracy. Although these technologies can improve user experiences and support decision-making processes, they also raise concerns regarding privacy violations, unauthorized data collection, and the manipulation of public opinion (Türegün, 2025).

One of the most significant examples of data exploitation in the digital age is the Cambridge Analytica scandal. The case attracted global attention in 2018 after revelations that personal data from millions of Facebook users had been harvested without proper consent and used to create psychographic profiles for political advertising. Through micro-targeting techniques, political messages were tailored to specific groups of voters based on their psychological traits and behavioral patterns. This practice raised concerns about the ethical use of personal data, the integrity of democratic processes, and the potential for digital technologies to influence political behavior.

Several previous studies have examined the Cambridge Analytica scandal from different perspectives. Hinds et al. (2020) focused on privacy concerns and public perceptions following the unauthorized use of Facebook users' personal data, highlighting issues related to online privacy, trust, and users' understanding of data-driven algorithms. Meanwhile, Boldyreva et al. (2018) analyzed the ethical and political implications of the scandal, emphasizing the role of Big Data, psychographic profiling, and online manipulation in influencing political decision-making processes. Although these studies provide valuable insights into privacy and political ethics, they primarily concentrate on individual privacy concerns and the ethical consequences of political manipulation. Limited attention has been given to examining the Cambridge Analytica case through the Human Security framework proposed by the United Nations Development Programme (UNDP, 1994). Consequently, a research gap remains regarding how personal data exploitation, psychographic profiling, and digital psychological manipulation may constitute threats to political security, personal security, and community security in the digital era.

The Cambridge Analytica case demonstrates that security threats in the digital era extend beyond traditional concerns such as military conflict or physical violence. Modern threats increasingly involve the misuse of information, privacy violations, digital surveillance, and psychological manipulation. These challenges directly affect individuals and communities, making them relevant to the concept of Human Security introduced by UNDP. Human Security emphasizes the protection of individuals from various threats that endanger their freedom, dignity, and well-being.

Among the seven dimensions of Human Security proposed by UNDP, the Cambridge Analytica case is particularly relevant to political security, personal security, and community security. The exploitation of personal data threatens individual privacy and autonomy, while the use of psychographic targeting may influence political decision-making and contribute to social polarization. Therefore, the case provides an important opportunity to examine how digital technologies can create new forms of threats to human security in contemporary society.

Therefore, this study aims to analyze the Cambridge Analytica case using the Human Security framework introduced by UNDP in 1994. By examining the implications of data exploitation, psychographic profiling, and digital psychological manipulation, this research seeks to identify how the case reflects threats to political security, personal security, and community security. Furthermore, this study contributes to the existing literature by extending previous discussions on privacy and political ethics toward a broader Human Security perspective in the context of digital-era threats.

2. Theoretical Framework

2.1. Human Security Framework

The concept of Human Security was introduced by the United Nations Development Programme (UNDP) in the Human Development Report 1994 as a people-centered approach to security that focuses on protecting individuals rather than solely emphasizing state sovereignty or military power (UNDP, 1994). This approach broadens the traditional understanding of security by recognizing that threats to human well-being may arise not only from armed conflict but also from political oppression, economic instability, social conflict, environmental degradation, violence, and violations of personal rights and freedoms (UNDP, 1994; United Nations Human Security Unit, 2016). As a people-centered framework, Human Security

emphasizes the protection of human life, dignity, and quality of life while ensuring that individuals are free from conditions that threaten their safety and well-being (UNDP, 1994; United Nations Human Security Unit, 2016). To explain the multidimensional nature of security, UNDP identified seven dimensions of Human Security: economic security, food security, health security, environmental security, personal security, community security, and political security (UNDP, 1994). These dimensions demonstrate that security threats can emerge from social, economic, political, environmental, and technological factors that directly affect human welfare and are closely interconnected (Schlotzhauer, 2010; Bindenagel Šehović, 2018).

In the digital era, the Human Security framework has become increasingly relevant because technological developments have introduced new forms of threats, including data exploitation, digital surveillance, disinformation, and psychological manipulation through online platforms. These threats directly affect individuals and communities by influencing privacy, autonomy, social cohesion, and democratic participation. The Cambridge Analytica case illustrates how personal data can be collected, analyzed, and utilized to influence political behavior and shape public opinion through psychographic profiling and micro-targeting strategies. Such practices demonstrate that contemporary security threats extend beyond physical and military concerns, making Human Security a useful framework for understanding how digital technologies may create risks to individual freedom, community stability, and political processes in modern society (UNDP, 1994; United Nations Human Security Unit, 2016).

2.2. Relevant Dimensions of Human Security

Among the seven dimensions of Human Security proposed by the United Nations Development Programme, this study focuses on political security, personal security, and community security because these dimensions are the most relevant to the Cambridge Analytica case. Political security refers to the protection of individuals' political rights and freedoms from oppression, manipulation, and abuse of power, ensuring that people can participate freely in political processes without fear of discrimination, intimidation, or violations of human rights (UNDP, 1994; United Nations Human Security Unit, 2016). This dimension is closely associated with freedom of expression, access to accurate information, democratic participation, and protection from political repression (United Nations Human Security Unit, 2016). Personal security concerns the protection of individuals from physical, psychological, and emotional threats that may endanger their safety and well-being, including violence, crime, human rights violations, privacy breaches, digital surveillance, cyber harassment, and psychological manipulation in online environments (UNDP, 1994; United Nations Human Security Unit, 2016). Meanwhile, community security focuses on protecting social groups, cultural identity, and social cohesion from threats that may create conflict, discrimination, social fragmentation, ethnic tensions, or social violence, while maintaining harmonious relationships within society (UNDP, 1994; United Nations Human Security Unit, 2016).

In today's digital environment, the dimensions of political, personal, and community security are increasingly exposed to emerging risks driven by the extensive use of social media, algorithmic systems, and data-intensive technologies. Political security is particularly vulnerable to practices such as targeted political advertising, misinformation campaigns, and behavioral influence techniques that can shape electoral choices and public opinion. Personal security is challenged by the extensive collection and processing of individual data, which may compromise privacy rights, personal autonomy, and control over one's own information. Meanwhile, community security is affected by algorithmic content filtering that tends to expose users to information aligned with their existing views, contributing to social fragmentation and deeper political divisions. The Cambridge Analytica scandal demonstrates how personal information and psychographic analysis can be leveraged to influence citizens, exploit psychological characteristics, and reinforce divisions among social groups. As a result, such practices pose significant challenges to democratic values, individual freedoms, and social cohesion within contemporary societies (UNDP, 1994; United Nations Human Security Unit, 2016).

2.3. Digital Psychological Manipulation , Micro-targeting, and Psychographic Profiling

Digital psychological manipulation refers to the use of digital technologies, algorithms, and personal data to influence individuals' thoughts, emotions, attitudes, and behavior in online environments (Bakir, 2020). This form of manipulation commonly occurs through social media platforms, targeted

advertisements, personalized content, and algorithm-driven recommendations designed to shape user perceptions and decision-making processes. Advances in Big Data analytics and artificial intelligence have enabled organizations to collect and analyze large amounts of personal information, allowing messages to be tailored according to users' psychological characteristics, interests, and online behavior. In many cases, digital psychological manipulation exploits cognitive biases, emotional reactions, and users' limited awareness of how digital platforms operate, making it an increasingly influential tool for shaping public opinion and behavior in the digital era (Bakir, 2020).

Two key techniques associated with digital psychological manipulation are micro-targeting and psychographic profiling. Micro-targeting refers to the delivery of highly personalized messages or advertisements to specific groups of individuals based on their personal data, preferences, demographic characteristics, and behavioral patterns, while psychographic profiling involves analyzing individuals' personalities, emotions, values, and psychological traits to predict how they may respond to particular messages (Bakir, 2020). These techniques enable organizations to develop highly customized communication strategies that influence political attitudes and decision-making processes. The Cambridge Analytica case represents one of the most significant examples of this practice, where personal data collected from Facebook users were analyzed to create psychographic profiles and subsequently used to deliver targeted political advertisements during the Brexit referendum and the 2016 United States presidential election. This case demonstrates how digital technologies can be utilized not only for communication but also as powerful instruments of psychological influence, political manipulation, and behavioral control through highly personalized political messaging (Cadwalladr & Graham-Harrison, 2018; Bakir, 2020).

3. Method

This study employs a qualitative research design to examine the Cambridge Analytica scandal through the Human Security framework. According to Creswell (2013), qualitative research is an interpretive approach that seeks to understand social phenomena by exploring events, experiences, and human behavior within their natural contexts. Qualitative inquiry enables researchers to analyze complex social realities that cannot be adequately understood through numerical measurements alone (Creswell, 2013). This approach is particularly appropriate for the present study because the Cambridge Analytica case involves multidimensional issues, including data exploitation, psychological manipulation, political influence, privacy violations, and digital security, all of which require contextual and interpretive analysis.

The study adopts a case study approach to investigate the Cambridge Analytica scandal as a contemporary phenomenon occurring within a real-world socio-political and technological environment. Yin (2018) argues that case study research is suitable when researchers seek to understand complex contemporary events in which the boundaries between the phenomenon and its context are not clearly defined. The Cambridge Analytica case represents a critical and influential example of data-driven political manipulation, making it an appropriate case for examining how digital technologies can generate threats to Human Security. Through this approach, the research explores the mechanisms of personal data exploitation, psychographic profiling, and micro-targeting, as well as their implications for political, personal, and community security.

Data collection was conducted through a literature review and document analysis. The study utilized secondary data obtained from peer-reviewed academic journals, books, official reports, investigative journalism articles, policy documents, and institutional publications related to Human Security, digital psychological manipulation, data exploitation, and the Cambridge Analytica scandal. Key sources included the Human Development Report 1994 published by the United Nations Development Programme (UNDP), reports from the United Nations Human Security Unit, investigative reports from The Guardian and The New York Times, and scholarly publications discussing psychographic profiling, political micro-targeting, digital campaigns, privacy issues, and threats to democratic processes. The use of multiple sources allowed the researcher to compare and verify information from different perspectives, thereby enhancing the credibility and reliability of the findings.

The collected data were analyzed using descriptive qualitative analysis guided by the Human Security framework proposed by UNDP (1994). The analysis process consisted of three stages. First, relevant information regarding data exploitation, psychographic profiling, micro-targeting practices, and their

social impacts was identified and organized from the collected sources. Second, the data were categorized according to the Human Security dimensions most relevant to the case, namely political security, personal security, and community security (UNDP, 1994). Third, an interpretive analysis was conducted to examine how the activities and outcomes associated with Cambridge Analytica constituted threats to these dimensions of Human Security. This analytical process enabled the study to move beyond a descriptive account of the scandal and provide a theoretically grounded assessment of its implications for democratic participation, individual autonomy, privacy protection, and social cohesion in the digital era.

To strengthen the validity of the analysis, data triangulation was applied by comparing information derived from academic literature, official institutional reports, and investigative journalism sources. This approach helped minimize potential bias from any single source and ensured a more comprehensive understanding of the case. Through the integration of qualitative case study methods and the Human Security framework, this research aims to provide a systematic assessment of how digital technologies and data-driven political strategies can create emerging threats to individuals and communities in contemporary society.

4. Results and Discussion

4.1. Chronolgy of the Cambridge Analytica Case

The literature analysis shows that implementing strong communication security in UAV systems introduces significant challenges because UAV platforms commonly operate under constrained computational conditions. UAV systems generally utilize lightweight embedded processors with limited memory capacity, restricted computational capability, finite battery resources, and constrained communication bandwidth (Roman et al., 2016).

This study employs comparative literature analysis to evaluate the effectiveness of ASCON lightweight cryptography for secure UAV surveillance communications. It identifies significant cybersecurity risks faced by UAV systems, including spoofing and eavesdropping, which threaten operational integrity and communication authenticity. Traditional cryptographic methods often prove inadequate for resource-constrained UAV environments due to high computational demands. ASCON's design, featuring Authenticated Encryption with Associated Data (AEAD), offers advantages such as simultaneous secrecy, integrity, and authentication, making it suitable for low-power devices. The findings suggest ASCON provides robust protection against unauthorized access and manipulations, ultimately presenting it as an optimal choice for real-time secure communications in UAV settings. While this analysis is limited to literature review, it highlights ASCON's potential for future research, particularly in practical implementations and performance evaluations.

4.2. Mechanism of Data Exploitation

The data exploitation mechanism used by Cambridge Analytica relied on the large-scale collection and analysis of personal data obtained through Facebook. The process began with the “This Is Your Digital Life” application developed by Aleksandr Kogan, which appeared as a personality quiz for Facebook users (Rosenberg et al., 2018). Although only around 270,000 users directly installed the application, Facebook’s Open Graph API at the time allowed the application to access not only the data of users who installed it, but also information from their Facebook friends without explicit consent. As a result, data from approximately 87 million users were collected (Rosenberg et al., 2018).

The harvested data included users’ personal profiles, liked pages, online interests, locations, social interactions, and behavioral patterns. These data were then analyzed using psychographic profiling techniques to identify users’ psychological characteristics, personality traits, emotional tendencies, and political preferences (Rosenberg et al., 2018; Bakir, 2020). Cambridge Analytica reportedly applied the OCEAN personality model, which consists of openness, conscientiousness, extraversion, agreeableness, and neuroticism, to classify individuals based on their psychological behavior (Bakir, 2020).

After the profiling process, the collected information was used for micro-targeting strategies in political campaigns. Specific political advertisements and messages were tailored according to users’ psychological profiles and distributed through digital platforms such as Facebook (Bakir, 2020).

Individuals considered emotionally vulnerable or politically undecided received highly personalized political content designed to influence their perceptions and voting behavior. In addition, Cambridge Analytica also applied voter suppression strategies by targeting groups likely to support opposing candidates and exposing them to negative or demotivating political content to reduce voter participation (Bakir, 2020).

This mechanism demonstrates that the Cambridge Analytica scandal was not a conventional cyberattack involving malware or system intrusion, but rather a form of digital exploitation that utilized personal data, algorithmic analysis, and psychological manipulation to influence public opinion and democratic processes. The case also reflects how personal data can be transformed into a political weapon in the digital era (Rosenberg et al., 2018; Bakir, 2020).

4.3. Analysis Based on Human Security

From the perspective of Human Security, the Cambridge Analytica scandal illustrates that contemporary threats to individuals are no longer limited to physical violence, armed conflict, or direct coercion. Instead, digital technologies have enabled new forms of influence that operate through the collection of personal data, psychological profiling, and algorithm-driven communication. The case demonstrates that data can be transformed into a strategic instrument for shaping perceptions, influencing political behavior, and reinforcing social divisions. Consequently, the Cambridge Analytica scandal should not be viewed solely as a privacy breach but as a multidimensional Human Security issue that affected political, personal, and community security.

4.3.1. Political Security

Political security was the most directly affected dimension in the Cambridge Analytica case. According to the UNDP Human Security framework, political security seeks to ensure that individuals can exercise their political rights and participate freely in democratic processes without manipulation, oppression, or abuse of power. In this case, the use of psychographic profiling and micro-targeting challenged these principles by enabling political actors to deliver highly personalized messages designed to influence specific groups of voters.

Unlike conventional political campaigns that communicate publicly and transparently, micro-targeting operates in a largely invisible manner, making it difficult for citizens, regulators, and even opposing political actors to scrutinize the information being distributed. This creates an imbalance in the democratic process because voters may be exposed to customized narratives specifically designed to exploit their fears, emotions, and psychological characteristics. As a result, political decisions may no longer be based primarily on informed deliberation but instead on carefully engineered emotional responses.

Furthermore, reports regarding voter suppression strategies suggest that some targeted communications were intended not only to persuade voters but also to discourage political participation among specific groups. Such practices undermine democratic equality by selectively influencing who participates in elections and how political choices are formed. Therefore, the Cambridge Analytica case represents a significant threat to political security because it compromised political autonomy, transparency, and the integrity of democratic decision-making processes.

4.3.2. Personal Security

The scandal also constituted a serious threat to personal security through the unauthorized collection, analysis, and exploitation of personal data. Within the Human Security framework, personal security involves protecting individuals from threats that undermine their safety, dignity, freedom, and autonomy. In the digital age, personal information has become an extension of individual identity because it reflects personal preferences, beliefs, behaviors, and social relationships.

The collection of data from millions of Facebook users without meaningful consent violated individuals' ability to control their own personal information. More importantly, the data were not merely stored or analyzed for commercial purposes but were utilized to develop psychological profiles that could

predict and influence behavior. This transformed personal data into a mechanism of behavioral intervention, raising concerns about individual autonomy and freedom of thought.

The case also highlights how excessive trust in digital platforms can become a Human Security vulnerability. Many users voluntarily provided access to personal information without fully understanding how that information could be processed, shared, or exploited. Consequently, the threat was not limited to privacy violations alone but extended to the erosion of individuals' capacity to make independent decisions free from hidden psychological influence. From this perspective, the Cambridge Analytica scandal demonstrates that personal security in the digital era increasingly depends on the protection of personal data and informational self-determination.

4.3.3. Community Security

Community security was also significantly affected through the reinforcement of social fragmentation and political polarization. Community security focuses on preserving social cohesion, mutual trust, and harmonious relationships among members of society. However, the data-driven communication strategies employed by Cambridge Analytica contributed to the creation of fragmented information environments in which different groups were exposed to different political narratives based on their psychological profiles.

Algorithmic personalization and micro-targeting can encourage the formation of echo chambers, where individuals primarily encounter information that confirms their existing beliefs while limiting exposure to alternative perspectives. This process strengthens ideological divisions and reduces opportunities for constructive dialogue between groups with differing viewpoints. Over time, such conditions can weaken social cohesion and increase distrust among communities.

The Cambridge Analytica case demonstrates that digital technologies are capable of amplifying societal divisions by exploiting emotional and psychological differences among citizens. Rather than promoting informed public discourse, targeted communication strategies may encourage polarization and antagonism between social groups. Consequently, the case represents a threat to community security because it undermines social unity, fosters division, and weakens the collective trust necessary for democratic societies to function effectively.

4.4. Analysis of Human Vulnerabilities

The Cambridge Analytica case demonstrates that the primary vulnerability in modern digital systems does not always originate from sophisticated hacking techniques or technical cyberattacks, but rather from human behavior and psychological weaknesses. One of the main vulnerabilities identified in this case was blind trust toward digital platforms and third-party applications. Many Facebook users granted access permissions to applications such as “This Is Your Digital Life” without fully understanding how their personal data would be collected, processed, and utilized. This behavior reflects low awareness of digital privacy and limited understanding of data protection risks in online environments.

Human vulnerability was also intensified through psychological manipulation strategies. Cambridge Analytica utilized psychographic profiling and micro-targeting techniques to exploit users’ emotions, fears, beliefs, and political preferences. By analyzing behavioral patterns and psychological characteristics, personalized political messages could be delivered to influence individuals more effectively. This shows that in the digital era, psychological vulnerabilities can become strategic targets for political and social manipulation through algorithm-driven platforms.

In addition to human vulnerabilities, the case also exposed weaknesses within digital systems and algorithms. Facebook’s algorithmic system was primarily designed to maximize user engagement and interaction without sufficient ethical control mechanisms. As a result, the platform failed to prevent the large-scale exploitation of personal data conducted by third parties. The absence of strict oversight and transparency regarding data collection practices created opportunities for misuse of personal information on a massive scale.

Despite these vulnerabilities, the case also highlighted an important aspect of human strength. The scandal was eventually exposed through the actions of Christopher Wylie, a former Cambridge Analytica

data scientist who decided to reveal the company's internal practices to the public. Wylie's decision reflected the role of human conscience and ethical awareness in confronting the misuse of digital technologies. His whistleblowing actions demonstrated that human integrity can serve as a critical safeguard when digital systems, corporate ethics, and regulatory mechanisms fail to protect individuals and democratic values.

4.5. Mitigation and Solutions

The Cambridge Analytica scandal demonstrates the urgent need for stronger protection mechanisms against digital data exploitation and psychological manipulation in online environments. One of the primary mitigation efforts is the improvement of digital literacy and public awareness regarding personal data protection. Many users involved in the case granted application permissions without fully understanding the risks associated with third-party data access. Therefore, individuals need to develop a better understanding of privacy policies, digital consent, and the potential misuse of personal information on social media platforms.

In addition to user awareness, social media companies must strengthen transparency and accountability in data management practices. Digital platforms such as Facebook should implement stricter controls over third-party applications, limit unnecessary data access, and improve monitoring systems to detect suspicious data collection activities. Algorithmic systems that prioritize engagement without ethical considerations also require stronger oversight mechanisms to reduce the spread of manipulative political content, disinformation, and echo chambers.

Regulatory and legal frameworks also play a crucial role in mitigating similar threats in the future. Governments and international institutions need to establish stronger data protection regulations that ensure transparency, user consent, and accountability for organizations that collect and process personal data. The implementation of stricter privacy laws, such as limitations on political micro-targeting and psychographic profiling, can help reduce the misuse of digital platforms for political manipulation. In addition, independent oversight institutions are necessary to supervise digital campaign practices and ensure the protection of democratic processes.

Another important mitigation effort involves strengthening ethical standards in the development and use of digital technologies. Companies involved in data analytics, artificial intelligence, and political advertising should adopt ethical guidelines that prioritize human rights, privacy protection, and democratic integrity. The Cambridge Analytica case illustrates that technological advancement without ethical responsibility can create significant threats to Human Security, particularly political security, personal security, and community security.

Finally, the role of whistleblowers, journalists, and civil society remains essential in identifying and exposing unethical digital practices. The disclosure of the Cambridge Analytica scandal by Christopher Wylie and investigative journalists demonstrated the importance of transparency and public accountability in the digital era. Strengthening legal protections for whistleblowers and supporting independent journalism can contribute to preventing future abuses of personal data and digital manipulation.

5. Conclusion

The study analyzed the Cambridge Analytica case using the Human Security framework introduced by the United Nations Development Programme (UNDP) in 1994. The findings demonstrate that the Cambridge Analytica scandal represents a contemporary form of human security threat in the digital era, where personal data exploitation, psychographic profiling, and micro-targeting techniques were utilized to influence individual behavior and political decision-making processes.

Based on the analysis, the case primarily affected three dimensions of Human Security: political security, personal security, and community security. Political security was threatened through the manipulation of voter behavior and democratic processes using highly personalized political messages. Personal security was compromised by the unauthorized collection and exploitation of personal data, resulting in violations of privacy, autonomy, and individual freedom. Meanwhile, community security was

affected by the creation of echo chambers and the intensification of social and political polarization, which weakened social cohesion within society.

The study also reveals that human vulnerability remains one of the most critical factors in digital security. Limited awareness of privacy risks, excessive trust in digital platforms, and susceptibility to psychological manipulation enabled large-scale data exploitation to occur. Furthermore, weaknesses in platform governance and insufficient regulatory oversight contributed to the misuse of personal information for political purposes.

The Cambridge Analytica case highlights that security threats in the digital age extend beyond traditional military and physical threats. Digital technologies can be used as instruments of psychological influence, political manipulation, and social fragmentation, creating significant risks to human well-being and democratic values. Therefore, strengthening digital literacy, improving data protection regulations, increasing platform accountability, and promoting ethical standards in the development of digital technologies are essential to safeguarding Human Security in contemporary society.

Future research may further explore the impact of emerging technologies such as artificial intelligence, algorithmic recommendation systems, and large-scale data analytics on Human Security dimensions in order to better understand evolving digital threats and develop more effective protection strategies.

References

Bakir, V. (2020). Psychological operations in digital political campaigns: Assessing Cambridge Analytica's psychographic profiling and targeting. *Frontiers in Communication, 5*, 1–16. https://doi.org/10.3389/fcomm.2020.00067

Bindenagel Šehović, A. (2018). Introduction: Origins of human security. In A. Bindenagel Šehović, *Reimagining state and human security beyond borders* (pp. 1–29). Palgrave Pivot. https://doi.org/10.1007/978-3-319-72068-5_1

Boldyreva, E. L., Grishina, N. Y., & Duisembina, Y. (2018). Cambridge Analytica: Ethics and online manipulation with decision-making process. In *The European Proceedings of Social & Behavioural Sciences (EpSBS): 18th PCSF 2018 – Professional Culture of the Specialist of the Future* (pp. 70–79). https://doi.org/10.15405/epsbs.2018.12.02.10

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Congge, U., Guillamón, M. D., Nurmandi, A., Salahudin, & Sihidi, I. T. (2023). Digital democracy: A systematic literature review. *Frontiers in Political Science, 5*. https://doi.org/10.3389/fpos.2023.972802

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). SAGE Publications.

Federal Trade Commission. (2019, July 24). *FTC sues Cambridge Analytica, settles with former CEO and app developer: FTC alleges they deceived Facebook users about data collection* [Press release]. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies, 143*, 102498. https://doi.org/10.1016/j.ijhcs.2020.102498

Kim, D. H., & Ellison, N. B. (2022). From observation on social media to offline political participation: The social media affordances approach. *New Media & Society, 24*(12). https://doi.org/10.1177/1461444821998346

Lorenz-Spreen, P., Oswald, L., Lewandowsky, S., & Hertwig, R. (2022). A systematic review of worldwide causal and correlational evidence on digital media and democracy. *Nature Human Behaviour*. https://doi.org/10.1038/s41562-022-01460-1

Memoli, M., & Schecter, A. (2018, April 26). Bannon turned Cambridge into "propaganda machine," whistleblower says. *NBC News*. https://www.nbcnews.com/politics/politics-news/bannon-turned-cambridge-propaganda-machine-whistleblower-says-n869086

Neuman, S., & Dwyer, C. (2018, March 20). Cambridge Analytica CEO suspended one day after release of hidden camera report. *NPR*. https://www.npr.org/2018/03/20/595338507/cambridge-analytica-ceo-suspended-one-day-

after-release-of-hidden-camera-report

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). How Trump consultants exploited the Facebook data of millions. *The New York Times*. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Schlotzhauer, N. (2010). Human security: Assessing the literature. *Regional Development Dialogue, 31*(1), 1–17.

Türegün, N. (2025). Digital transformation and cybersecurity risks. *International Journal of Accounting Information Systems, 56*. https://doi.org/10.1016/j.accinf.2025.100749

United Nations Development Programme. (1994). *Human development report 1994: New dimensions of human security*. Oxford University Press.

United Nations Human Security Unit. (2016). *Human security handbook: An integrated approach for the realization of the Sustainable Development Goals and the priority areas of the international community and the United Nations system*.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.