Journal of Governance and Public Administration (JoGaPA)
Volume 1, No 3 – Juni 2024
e-ISSN : 3031-7584

FROM SOCIAL MEDIA TO THE DEFENSE FIELD: AN EXPLORATION OF GEN Z'S ROLE IN NATIONAL SECURITY

Aris Sarjito[1]*
[1]Republic of Indonesia Defense University, Indonesia
[1]arissarjito@gmail.com

Received: 28-06- 2024	Revised: 20-06-2024	Approved: 25-06-2024

ABSTRACT

This study explores the integration of Gen Z into national security frameworks, focusing on their potential contributions to cybersecurity and intelligence. With their digital nativeness and unique skill sets, Gen Z individuals are poised to address contemporary cyber threats effectively. The aim of this research is to investigate the key digital competencies of Gen Z, their role in enhancing national security operations, and the ethical and practical challenges of integrating them into defense roles. Utilizing qualitative research methods, the study employs secondary data from recent literature and industry reports to analyze these aspects. Research findings indicate that Gen Z's proficiency in digital technologies and social media can significantly bolster national security operations. Moreover, their inclusion in cybersecurity and intelligence roles is crucial for adapting to evolving threats. However, the integration process presents ethical dilemmas and practical challenges, such as balancing privacy concerns with security needs and adapting existing frameworks to accommodate the new generation's working styles. The conclusion underscores the necessity of leveraging Gen Z's competencies while addressing integration challenges to strengthen national defense. This study provides insights into the strategic importance of Gen Z in national security, offering a foundation for future policies and practices.

Keywords: cybersecurity, digital competencies, Generation Z, intelligence roles, national security

INTRODUCTION

The rapid advancement of technology and the pervasive influence of social media have significantly shaped the characteristics and behaviors of Generation Z (Gen Z). This generation, born between the mid-1990s and early 2010s, has grown up in a digitally connected world, making them distinct from previous generations in various ways (Holton & Fraser, 2015). This research explores the state-of-the-art research on how Gen Z's unique characteristics, particularly their digital fluency and social media engagement, can be leveraged in the field of national security.

Gen Z is often referred to as a digital native, having been exposed to technology from a very young age. According to a study by the Pew Research Center, over 95% of Gen Z individuals own a smartphone and spend a significant portion of their day online (Pew Research Center, 2019). This constant connectivity has fostered a generation that is highly adept at navigating digital landscapes and utilizing various social media platforms.

Moreover, Gen Z is known for its preference for visual and interactive content, often favoring platforms like Instagram, TikTok, and YouTube over traditional text-based media (Anderson & Jiang, 2018). Their ability to quickly adapt to new technologies and trends makes them a valuable asset in fields that require rapid information processing and dissemination, such as national security.

Social media has become a critical tool in national security for monitoring, communication, and information dissemination. Platforms like Twitter and Facebook are frequently used for open-source intelligence (OSINT), where analysts gather publicly available information to assess security threats (Omand et al., 2019). Gen Z's inherent proficiency with these platforms can enhance the effectiveness of OSINT operations.

Additionally, social media is instrumental in shaping public opinion and disseminating information during crises. Gen Z's familiarity with creating and spreading content can be harnessed to manage public communication strategies effectively. For instance, during the COVID-19 pandemic, young influencers on platforms like TikTok played a significant role in spreading public health messages (Basch et al., 2022). Similar strategies can be applied in national security to quickly and effectively communicate with the public.

Another critical area where Gen Z's skills can be pivotal is cybersecurity. As the frequency and sophistication of cyber threats increase, there is a growing need for cybersecurity professionals who can anticipate and counteract these threats. Gen Z's early exposure to technology and their interest in digital fields position them well to fill this gap.

Educational institutions and governments are recognizing this potential and are increasingly offering programs and initiatives to attract young people into cybersecurity careers. For example, the U.S. Department of Homeland Security has launched several initiatives aimed at developing the next generation of cybersecurity professionals (DHS, 2021). Encouraging Gen Z to pursue careers in this field can significantly bolster national security efforts.

While leveraging Gen Z's digital skills offers numerous benefits, it also presents ethical considerations and challenges. The reliance on social media for national security purposes raises privacy concerns, as monitoring platforms can infringe on individual rights (Lipschultz, 2020). Furthermore, the spread of misinformation and the potential for digital manipulation pose significant risks.

Addressing these challenges requires a balanced approach that respects privacy while ensuring security. Education and training programs for Gen Z must emphasize ethical considerations in digital practices, ensuring that they are equipped to navigate these complexities responsibly (Floridi & Taddeo, 2016).

The study, "From Social Media to the Defense Field: An Exploration of Gen Z's Role in National Security," investigates the emerging influence of Gen Z within the realm of national defense. This research is critical given the unique characteristics and technological fluency of Gen Z, who have grown up in an era dominated by social media and digital connectivity. Understanding their potential roles and contributions to national security frameworks is essential for developing effective strategies in an increasingly digitized world.

A thorough literature review supports this study, drawing from recent journal articles and conference proceedings published within the last five years. This review not only covers theoretical perspectives but also includes empirical evidence to provide a comprehensive foundation for the research.

Recent studies highlight the importance of integrating younger generations into cybersecurity and intelligence roles. According to (Tirocchi et al., 2022), Gen Z's digital nativeness positions them uniquely to understand and counter cyber threats. This theoretical perspective is echoed by (Scott-Tarman, 2023), who emphasize the need for national security frameworks to evolve in response to the generational shift.

Empirical research has demonstrated the practical implications of involving Gen Z in national security. For instance, a study by (Takács & Pogátsnik, 2024) found that Gen Z individuals bring innovative problem-solving skills to cybersecurity roles, leveraging their familiarity with technology to develop novel defense strategies. Similarly, empirical evidence from (Wilson et al., 2022) indicates that Gen Z's adeptness at social media can be harnessed for intelligence gathering and analysis, providing new avenues for national defense agencies to explore.

Several efforts have been made to integrate Gen Z into national security roles effectively. For example, the Defense Advanced Research Projects Agency (DARPA) has initiated programs aimed at recruiting young talent directly from high schools and universities (Defense Advanced Research Projects Agency (DARPA), 2023). Additionally, collaborative efforts between educational institutions and defense agencies, such as the CyberCorps Scholarship for Service program, have been pivotal in bridging the skills gap in the cybersecurity workforce (National Science Foundation, 2022).

Recent conference proceedings also shed light on this topic. The 2022 International Conference on Cybersecurity (ICCS) featured numerous presentations on the role of Gen Z in cyber defense, highlighting both opportunities and challenges (ICCS, 2022). These discussions underline the importance of tailored training programs and the need for policy adaptations to accommodate the distinct characteristics of Gen Z.

Statement of the Problem

The rapid evolution of technology and the pervasive use of social media have significantly influenced the behaviors and skills of Generation Z (Gen Z). The constant interaction with digital platforms that shaped this generation, which was born between the middle of the 1990s and the beginning of the 2010s, has uniquely positioned them to make contributions to a variety of fields, including national security. However, the integration of Gen Z's digital fluency into national defense strategies remains unexplored. This research seeks to address the gap in understanding how Gen Z's characteristics and skills can be effectively leveraged in the defense field to enhance national security efforts.

Research Objectives

Its research goals are to look into Gen Z's digital skills and how they relate to national security, to find out what roles they might play in cybersecurity and intelligence for the national defense, and to find out what moral and practical problems come up when Gen Z is included in national security systems.

Research Questions

1. What specific digital competencies of Gen Z are most relevant to enhancing national security operations?

This question aims to identify and evaluate the particular digital skills that Gen Z possesses, such as social media proficiency, cybersecurity awareness, and data analysis capabilities. Understanding these competencies is crucial for determining how they can be applied effectively in national security contexts. Recent studies indicate that Gen Z's familiarity with digital platforms and technology could be a valuable asset for intelligence and security agencies (Anderson & Jiang, 2018; Pew Research Center, 2019).

2. How can Gen Z be integrated into cybersecurity and intelligence roles within national defense?

   This question focuses on exploring the practical ways in which Gen Z can be incorporated into cybersecurity and intelligence roles. It seeks to identify strategies for recruiting, training, and retaining Gen Z individuals in these critical areas. Given the increasing frequency of cyber threats, there is a pressing need to bolster cybersecurity defenses, and Gen Z's digital native status positions them well to contribute effectively (DHS, 2021; Floridi & Taddeo, 2016).
3. What ethical and practical challenges arise from integrating Gen Z into national security frameworks, and how can they be addressed?

   This question addresses the potential ethical and practical issues that may emerge when incorporating Gen Z into national security roles. These challenges may include privacy concerns, the risk of misinformation, and the need for ethical guidelines in digital practices. Addressing these concerns is essential for ensuring that Gen Z's contributions are both effective and ethically sound (Basch et al., 2022; Omand et al., 2019).

The integration of Gen Z's digital competencies into national security operations offers significant potential to enhance defense capabilities. By analyzing the specific skills of Gen Z, exploring their roles in cybersecurity and intelligence, and addressing the associated ethical and practical challenges, this research aims to provide a comprehensive understanding of how this generation can be effectively leveraged in the defense field. As we move forward, it is crucial to ensure that Gen Z's unique abilities are harnessed responsibly to strengthen national security efforts.

RESEARCH METHODS

Qualitative research methods provide an in-depth understanding of complex phenomena, making them particularly useful for exploring the nuanced roles of Generation Z (Gen Z) in national security. According to Creswell & Creswell (2017), secondary data analysis involves using data already gathered by previous researchers or institutions to answer new research questions. This essay outlines the application of qualitative research methods using secondary data to investigate the integration of Gen Z's digital competencies into national security strategies.

Qualitative research aims to uncover rich, detailed insights into social phenomena through methods such as interviews, focus groups, and content analysis (Creswell & Creswell, 2017). Secondary data analysis, a type of qualitative research, involves re-examining data originally collected for different purposes. This approach can include analyzing documents, archival records, social media content, and previous research studies. Using secondary data allows researchers to leverage existing information, saving time and resources while providing access to large datasets that may be otherwise unavailable (Sherif, 2018).

To explore Gen Z's role in national security through secondary data, researchers can analyze various data sources. For instance, social media content can provide valuable insights into the digital behaviors and competencies of Gen Z. Platforms like Twitter, Instagram, and TikTok contain vast amounts of user-generated content that reflect how Gen Z interacts with technology, communicates, and responds to security-related issues (Anderson & Jiang, 2018).

Additionally, government and institutional reports on cybersecurity and digital literacy programs can serve as rich sources of secondary data. These documents often

include statistical data, program evaluations, and policy analyses that can shed light on the current state of Gen Z's involvement in national security efforts (DHS, 2021). By examining these sources, researchers can identify trends, gaps, and opportunities for enhancing Gen Z's contributions to national defense.

Methods

Research Design: This study employs a qualitative research design utilizing secondary data to explore Gen Z's role in national security. This approach allows for an in-depth examination of existing data sources to understand patterns and themes relevant to the research questions (Brennen, 2021; Silverman, 2016).

Data Collection: Data collection focused on gathering and analyzing existing data from secondary sources such as social media posts, online forums, and previously published reports. This method provides insights into public perceptions and discourses relevant to Gen Z and national security (Heaton, 2008; Hsieh & Shannon, 2005).

Data Analysis: The analysis of secondary data involved thematic analysis to identify and interpret key themes and patterns within the data sources. This approach was essential for understanding the implications of Gen Z's perspectives on national security (Braun & Clarke, 2006; Guest et al., 2012).

Below is a visual representation of the method steps used in this research.

Figure 1: Methods

Source: proceed from various sources by author (2024)

Figure 1 illustrates the steps involved in the research methodology, including: (1) Research Design - a qualitative approach using secondary data; (2) Data Collection - comprising social media posts, online forums, and published reports; and (3) Data Analysis - employing thematic analysis.

The research design chosen allows for a deep exploration of Gen Z's attitudes and behaviors related to national security, while the data collection methods ensure a comprehensive gathering of relevant information from various sources. The use of thematic analysis in data analysis will help identify key patterns and trends in Gen Z's engagement with national security issues, providing valuable insights for policymakers and defense professionals. This research aims to bridge the gap between social media discourse and the defense field, shedding light on the potential role of Gen Z in shaping national security policies.

RESULTS AND DISCUSSION

1. Key Digital Competencies of Gen Z: Crucial for Enhancing National Security Operations

The digital era has given rise to Generation Z (Gen Z), a cohort known for their innate proficiency with technology. Born between the mid-1990s and early 2010s, Gen Z has grown up in a world where digital connectivity and social media are integral to daily life. This immersion in technology has endowed them with unique digital competencies

that can be highly relevant to national security operations (Katz et al., 2022). This discussion explores these competencies, specifically focusing on social media proficiency, cybersecurity awareness, and data analysis capabilities, and evaluates how they can be effectively applied in national security contexts.

Social Media Proficiency

Gen Z's proficiency with social media is one of their most distinguishing digital skills. They are adept at using platforms such as Twitter, Instagram, TikTok, and Snapchat to communicate, share information, and mobilize communities (Pritts, 2022). This skill can be leveraged in national security for both intelligence gathering and public communication.

For instance, social media can serve as a rich source of open-source intelligence (OSINT). According to Omand et al. (2019), social media intelligence (SOCMINT) can provide valuable insights into emerging threats, public sentiment, and potential security breaches. Gen Z's ability to navigate these platforms, identify trends, and analyze content can enhance the efficiency and accuracy of OSINT operations. Additionally, their familiarity with these platforms allows them to effectively disseminate information and counter misinformation during crises, thus supporting public communication strategies (Basch et al., 2022).

Cybersecurity Awareness

Another critical competency of Gen Z is their heightened awareness of cybersecurity. Gen Z has gained a thorough understanding of digital security procedures as a result of growing up in an era with frequent cyber threats and data breaches. This awareness is vital for national security operations, which increasingly depend on robust cybersecurity measures to protect sensitive information and infrastructure (Ozkaya, 2019).

Educational initiatives and programs have further strengthened Gen Z's cybersecurity skills. For example, the U.S. Department of Homeland Security has implemented initiatives aimed at fostering cybersecurity careers among young people (DHS, 2021). These programs equip Gen Z with knowledge of cybersecurity protocols, threat detection, and incident response. Integrating these young cybersecurity professionals into national defense teams can enhance the resilience and adaptability of cybersecurity operations, ensuring that they are well-prepared to address evolving cyber threats (Sarjito, 2024).

Data Analysis Capabilities

Data analysis is another area where Gen Z excels. The proliferation of big data has created a demand for individuals who can interpret and derive actionable insights from large datasets. Gen Z's comfort with technology and analytical tools positions them well to meet this demand. They are proficient in using software and programming languages like Python, R, and SQL to analyze data and identify patterns (Khadka, 2019).

In the context of national security, data analysis is crucial for intelligence and strategic decision-making. By analyzing data from various sources, including social media, surveillance, and public records, Gen Z can help identify potential security threats, predict trends, and develop informed strategies (Van Puyvelde et al., 2017). Their ability to handle and analyze large volumes of data can enhance the capabilities of national security agencies, making operations more data-driven and precise (Floridi & Taddeo, 2016).

Application in National Security Contexts

Understanding these digital competencies and their relevance to national security is essential for effectively integrating Gen Z into defense operations. Social media proficiency can be harnessed for both intelligence gathering and public communication, enhancing the ability to monitor and respond to security threats (Sciences et al., 2019). Cybersecurity awareness and skills are critical for protecting national infrastructure and responding to cyber incidents, while data analysis capabilities can improve the accuracy and efficiency of intelligence operations.

Moreover, fostering an environment that encourages the continuous development of these skills is vital. Providing training programs, creating opportunities for hands-on experience, and promoting collaboration between Gen Z and experienced security professionals can ensure that their digital competencies are fully utilized and further refined (Creswell & Creswell, 2017).

2. Integrating Gen Z into Cybersecurity and Intelligence Roles in National Defense

As cyber threats become increasingly sophisticated and pervasive, the need to strengthen national cybersecurity and intelligence capabilities is more critical than ever. Generation Z (Gen Z), with their innate digital proficiency, presents a unique opportunity to enhance these capabilities (Vogel, 2016). This discussion explores practical ways to integrate Gen Z into cybersecurity and intelligence roles within national defense by identifying strategies for recruiting, training, and retaining these digital natives.

Recruiting Gen Z into Cybersecurity and Intelligence Roles

Recruiting Gen Z into national defense roles begins with understanding their motivations and preferences. Gen Z values meaningful work, technological engagement, and opportunities for professional growth (Pew Research Center, 2019). To attract this generation, national defense organizations should highlight the impactful nature of cybersecurity and intelligence work and its critical role in protecting national security.

Innovative recruitment campaigns that leverage social media and digital platforms, where Gen Z spends significant time, can be particularly effective. For example, the U.S. Department of Homeland Security (DHS) has used social media to promote cybersecurity career opportunities, reaching potential candidates where they are most active (DHS, 2021). Collaborations with educational institutions to offer cybersecurity programs, internships, and career fairs can also facilitate recruitment by directly connecting with students interested in these fields.

Training Gen Z for Cybersecurity and Intelligence Roles

Once recruited, comprehensive and continuous training is essential to equip Gen Z with the skills needed for cybersecurity and intelligence roles. Given their digital native status, Gen Z individuals are likely to adapt quickly to technical training, but they also need specialized education to handle complex security challenges (Bower, 2020).

Training programs should include hands-on experience with the latest cybersecurity tools and technologies. Simulation-based training, where individuals can practice responding to cyberattacks in controlled environments, can be particularly effective (Hatzivasilis et al., 2020). Additionally, mentorship programs that pair Gen Z recruits with experienced cybersecurity professionals can provide valuable guidance and real-world insights.

Educational initiatives, such as the National Initiative for Cybersecurity Education (NICE) by the National Institute of Standards and Technology (NIST), offer frameworks for developing robust training programs that align with industry standards

and national security requirements (NIST, 2021). Encouraging participation in cybersecurity competitions and hackathons can also enhance practical skills and foster a culture of continuous learning and innovation.

Retaining Gen Z in Cybersecurity and Intelligence Roles

Retaining Gen Z in national defense roles requires addressing their career aspirations and ensuring job satisfaction. This generation values work-life balance, opportunities for advancement, and a supportive work environment (Twenge, 2017). National defense organizations must create a work culture that aligns with these values to retain talented individuals.

Offering clear career progression pathways and opportunities for professional development is crucial. Continuous education programs, advanced certifications, and leadership training can help Gen Z see a future within the organization (Maloni et al., 2019). Additionally, fostering a collaborative and inclusive work environment that values diversity and innovation can enhance job satisfaction and loyalty.

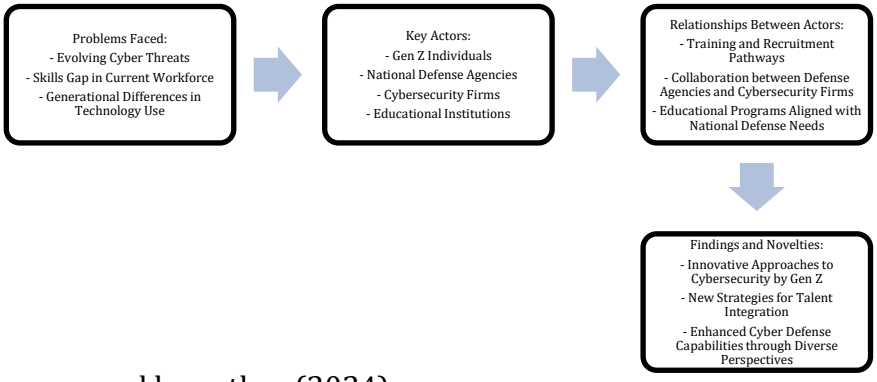
Recognizing and rewarding contributions through both monetary and non-monetary incentives can also motivate Gen Z employees. Flexible work arrangements, such as remote work options and flexible hours, can address their desire for work-life balance, making cybersecurity and intelligence roles more attractive (Deloitte, 2020).

Addressing Challenges and Ethical Considerations

Integrating Gen Z into cybersecurity and intelligence roles also requires addressing potential challenges and ethical considerations. The fast-evolving nature of cyber threats necessitates continuous adaptation and learning, which can be demanding. Providing mental health support and resources to manage stress and prevent burnout is essential (Burrell, 2023).

Ethically, the use of social media and digital surveillance in cybersecurity operations raises privacy concerns. Training programs must emphasize ethical guidelines and responsible practices to ensure that Gen Z professionals uphold the highest standards of integrity and respect for privacy (Floridi & Taddeo, 2016).

In this section, Figure 2 provides a schematic representation of the integration of Gen Z into cybersecurity and intelligence roles within national defense. This figure outlines the process, starting with the problems faced in current national defense strategies, identifying key actors involved, and illustrating the relationships between these actors. It then progresses to showcase the findings and novelties emerging from integrating Gen Z into these roles. This schematic aims to aid readers in understanding the study's approach and conceptual framework.



Source: proceed by author (2024)

Figure 2: Integrating Gen Z into Cybersecurity and Intelligence Roles in National Defense

This schematic figure helps to visually represent the framework for integrating Gen Z into national defense roles, illustrating the key elements and their interconnections. The findings and novelties section of the framework highlights the innovative approaches that Gen Z individuals bring to cybersecurity, as well as new strategies for integrating their talents into national defense roles. By incorporating diverse perspectives, the framework also aims to enhance overall cyber defense capabilities. This visual representation serves as a guide for educational institutions, defense agencies, and cybersecurity firms to collaborate effectively in aligning educational programs with national defense needs.

3. Addressing Ethical and Practical Challenges in Integrating Gen Z into National Security Frameworks

Integrating Generation Z (Gen Z) into national security frameworks presents both opportunities and challenges. While their digital proficiency and adaptability are valuable assets, there are significant ethical and practical challenges that must be addressed to ensure their contributions are effective and ethically sound (Trenerry et al., 2021). This discussion explores the primary ethical and practical issues, including privacy concerns, the risk of misinformation, and the need for ethical guidelines in digital practices, and proposes strategies to address these concerns.

Privacy Concerns

One of the most prominent ethical challenges in integrating Gen Z into national security roles is privacy. Given their deep involvement in digital and social media, Gen Z has a unique perspective on privacy, often balancing their desire for connectivity with a need for personal data protection (Slavtcheva-Petkova, 2023). However, their roles in national security might require them to engage in activities that can infringe on privacy, such as surveillance and data collection.

To address these concerns, it is essential to establish clear ethical guidelines that prioritize the protection of individual privacy while still allowing for effective security measures. Training programs should emphasize the importance of privacy and teach Gen Z professionals how to handle sensitive information responsibly. Transparency in data collection processes and adherence to legal frameworks, such as the General Data Protection Regulation (GDPR) in Europe and similar regulations elsewhere, are crucial to maintaining public trust and ethical standards (European Commission, 2018).

Risk of Misinformation

The proliferation of misinformation is another significant challenge. Gen Z, with their heavy reliance on social media for news and information, can be both perpetrators and victims of misinformation. In the context of national security, the spread of false information can have severe consequences, undermining public trust and complicating security operations (Hersman, 2020).

To mitigate this risk, comprehensive media literacy and critical thinking training should be integrated into the education and training programs for Gen Z in national security roles. This training should equip them with the skills to discern credible information from falsehoods and understand the implications of misinformation (Ireton & Posetti, 2018). Additionally, establishing robust verification protocols and promoting a culture of skepticism can help ensure that the information used in national security operations is accurate and reliable (Wardle & Derakhshan, 2017).

Need for Ethical Guidelines in Digital Practices

Gen Z's integration into national security also necessitates the development and enforcement of ethical guidelines for digital practices. The fast-paced nature of technological advancements can lead to ethical gray areas, particularly concerning the use of new surveillance technologies and artificial intelligence (AI) (Yazdi, 2021).

To address this, national security agencies must develop comprehensive ethical guidelines that cover various aspects of digital practices, including data collection, AI usage, and digital surveillance (Board, 2019). These guidelines should be regularly updated to keep pace with technological advancements and ensure that Gen Z professionals are aware of the ethical implications of their actions. Ethical training should be an ongoing process, with regular workshops and seminars to reinforce the importance of ethical behavior in national security operations (Floridi & Taddeo, 2016).

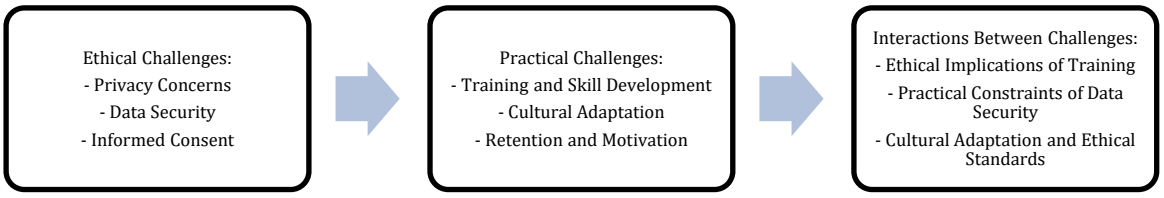
Practical Challenges

In addition to ethical issues, there are practical challenges in integrating Gen Z into national security roles. These include bridging the generational gap between Gen Z and older, more experienced security professionals, and ensuring that Gen Z's digital skills are effectively utilized (Georgescu & Bodislav, 2024).

To bridge the generational gap, fostering an inclusive and collaborative work environment is essential. Mentorship programs that pair Gen Z recruits with experienced professionals can facilitate knowledge transfer and mutual understanding. Encouraging open communication and valuing the contributions of all team members can also help create a cohesive workforce (Twenge, 2017).

Ensuring that Gen Z's digital skills are effectively utilized requires providing them with opportunities to apply their competencies in meaningful ways. This can be achieved through targeted assignments, continuous professional development, and involvement in cutting-edge projects. Recognizing and rewarding their contributions can also boost morale and retention rates (Deloitte, 2020).

Figure 3 illustrates the ethical and practical challenges associated with integrating Gen Z into national security frameworks. This schematic image outlines the key challenges, including issues related to ethical considerations, practical implementation, and the interactions between these aspects. It provides a visual representation to help readers understand the complexities and nuances of incorporating Gen Z into national security roles.



Source: proceed by author (2024)

Figure 3: The Ethical and Practical Challenges in Integrating Gen Z into National Security Frameworks

Figure 3 illustrates the ethical and practical challenges in integrating Gen Z into national security frameworks. It highlights three main areas: (1) Ethical Challenges such as balancing privacy concerns with surveillance, ensuring robust data security, and navigating informed consent in security roles; (2) Practical Challenges including the need to adapt training programs to Gen Z's learning styles, integrating their values with

existing protocols, and addressing issues related to career retention and motivation; and (3) Interactions Between Challenges that show how ethical considerations in training can impact effectiveness, how practical constraints of data security can affect operational efficiency, and how cultural adaptation must align with national security ethics. This figure provides a comprehensive view of the complexities involved in integrating Gen Z, offering insights into how these challenges interconnect and influence each other.

This schematic image provides a comprehensive view of the various ethical and practical challenges involved in integrating Gen Z into national security frameworks, illustrating the interconnections and areas of focus for addressing these challenges. By examining the ethical implications of training, including the impact of privacy concerns, national security agencies can ensure that their methods align with ethical standards. Additionally, balancing data security measures with operational efficiency is crucial for maintaining the integrity of sensitive information. By addressing these challenges and aligning Gen Z's values with national security ethics, agencies can effectively integrate the next generation into their frameworks while ensuring the highest level of security and satisfaction.

CONCLUSION

Generation Z's digital competencies, including social media proficiency, cybersecurity awareness, and data analysis capabilities, are highly relevant to enhancing national security operations. These skills, shaped by their upbringing in a digital world, offer significant potential for improving intelligence gathering, cybersecurity defenses, and data-driven decision-making. By effectively integrating these competencies into national security frameworks, agencies can leverage the unique strengths of Gen Z to address contemporary security challenges and build a more resilient defense infrastructure.

Gen Z's digital proficiency and adaptability make them ideal candidates for cybersecurity and intelligence roles within national defense. By implementing targeted recruitment strategies, providing comprehensive and continuous training, and fostering a supportive and inclusive work environment, national defense organizations can effectively integrate and retain Gen Z in these critical areas. Addressing the challenges and ethical considerations associated with these roles is also crucial to ensuring that Gen Z professionals contribute effectively and responsibly to national security efforts.

Integrating Gen Z into national security frameworks offers significant potential to enhance cybersecurity and intelligence capabilities. However, this integration must be carefully managed to address ethical and practical challenges, including privacy concerns, the risk of misinformation, and the need for ethical guidelines in digital practices. By establishing clear ethical standards, providing comprehensive training, and fostering an inclusive work environment, national security agencies can ensure that Gen Z's contributions are both effective and ethically sound. Addressing these challenges not only enhances the capabilities of national security operations but also builds a more resilient and trustworthy security infrastructure.

REFERENCE

Andersn, M., & Jiang, J. (2018). *Teens, Social Media & Technology 2018*. Pew Research Center. https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/

Basch, C. H., Hillyer, G. C., & Jaime, C. (2022). COVID-19 on TikTok: harnessing an emerging social media platform to convey important public health messages. *International Journal of Adolescent Medicine and Health*, *34*(5), 367–369.

Board, D. I. (2019). AI principles: recommendations on the ethical use of artificial intelligence by the department of defense: supporting document. *United States Department of Defense*.

Bower, J. D. (2020). *Generational Learning in the Marine Corps: The Importance of Information Age Thinking*.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Brennen, B. S. (2021). *Qualitative research methods for media studies*. routledge.

Burrell, D. N. (2023). *Real-World solutions for diversity, strategic change, and organizational development: perspectives in healthcare, education, business, and technology: Perspectives in Healthcare, Education, Business, and Technology*. IGI Global.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Defense Advanced Research Projects Agency (DARPA). (2023). Autonomous Systems in Modern Defense. *DARPA Research Papers*.

Deloitte. (2020). *Understanding Generation Z in the workplace*. Deloitte Insights. https://www2.deloitte.com/global/en/insights/focus/technology-and-the-future-of-work/understanding-generation-z-in-the-workplace.html

DHS. (2021). *Cybersecurity and Infrastructure Security Agency: National Initiative for Cybersecurity Careers and Studies. U.S. Department of Homeland Security*. https://www.cisa.gov/national-initiative-cybersecurity-careers-and-studies

European Commission. (2018). *General Data Protection Regulation (GDPR)*. European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en

Floridi, L., & Taddeo, M. (2016). What is data ethics? In *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* (Vol. 374, Issue 2083, p. 20160360). The Royal Society.

Georgescu, R. I., & Bodislav, D. A. (2024). The generational divide–A debate on technology and the decision-making process. *Theoretical and Applied Economics*, *31*(2 (639), Summer), 45–66.

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied thematic analysis*. sage.

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., & Leftheriotis, G. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences*, *10*(16), 5702.

Heaton, J. (2008). Secondary analysis of qualitative data. *The SAGE Handbook of Social Research Methods*, 506–519.

Hersman, R. (2020). *Wormhole Escalation in the New Nuclear Age (Summer 2020)*.

Holton, T., & Fraser, B. (2015). Generation Z and technology. *Defence Research and Development Canada*, *11*(3), 185–186.

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277–1288.

ICCS. (2022). Proceedings of the International Conference on Cybersecurity. *International Conference on Cybersecurity*.

Ireton, C., & Posetti, J. (2018). *Journalism, fake news & disinformation: handbook for*

journalism education and training. Unesco Publishing.

Katz, R., Ogilvie, S., Shaw, J., & Woodhead, L. (2022). *Gen Z, explained: The art of living in a digital age*. University of Chicago Press.

Khadka, B. (2019). *Data analysis theory and practice: Case: Python and Excel Tools*.

Lipschultz, J. H. (2020). *Social media communication: Concepts, practices, data, law and ethics*. Routledge.

Maloni, M., Hiatt, M. S., & Campbell, S. (2019). Understanding the work values of Gen Z business students. *The International Journal of Management Education*, *17*(3), 100320.

National Science Foundation. (2022). CyberCorps Scholarship for Service Program. *National Science Foundation*.

NIST. (2021). *National Initiative for Cybersecurity Education (NICE)*. National Institute of Standards and Technology. https://www.nist.gov/itl/applied-cybersecurity/nice

Omand, D., Bartlett, J., & Miller, C. (2019). Introducing social media intelligence (SOCMINT). In *Secret Intelligence* (pp. 77–94). Routledge.

Ozkaya, E. (2019). *Cybersecurity: the beginner's guide: a comprehensive guide to getting started in cybersecurity*. Packt Publishing Ltd.

Pew Research Center. (2019). *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*. Pew Research Center. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

Pritts, M. (2022). *Hey Girl, Feel my Thesis. Know what It's made of? Research Material*. Liberty University.

Sarjito, A. (2024). Optimizing Defense Management: Navigating the Impact of Conflict. *Manajemen Pertahanan: Jurnal Pemikiran Dan Penelitian Manajemen Pertahanan*, *10*(1), 97–119.

Sciences, N. A. of, Behavioral, D. of, Sciences, S., Behavioral, B. on, Sciences, S., Social, C. on a D. S. of, & Security, B. S. for A. to N. (2019). *A decadal survey of the social and behavioral sciences: A research agenda for advancing intelligence analysis*.

Scott-Tarman, J. (2023). *Changing the Guard: Preparing the Intelligence and National Security Community for the Generation Z Officer*. Archway Publishing.

Sherif, V. (2018). Evaluating preexisting qualitative research data for secondary analysis. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *19*(2).

Silverman, D. (2016). Introducing qualitative research. *Qualitative Research*, *3*(3), 14–25.

Slavtcheva-Petkova, V. (2023). *Young People, Media and Politics in the Digital Age*. Taylor & Francis.

Takács, J. M., & Pogátsnik, M. (2024). The Presence of Cybersecurity Competencies in the Engineering Education of Generation Z. *Acta Polytechnica Hungarica*, *21*(6).

Tirocchi, S., Scocco, M., & Crespi, I. (2022). Generation Z and cyberviolence: between digital platforms use and risk awareness. *International Review of Sociology*, *32*(3), 443–462.

Trenerry, B., Chng, S., Wang, Y., Suhaila, Z. S., Lim, S. S., Lu, H. Y., & Oh, P. H. (2021). Preparing workplaces for digital transformation: An integrative review and framework of multi-level factors. *Frontiers in Psychology*, *12*, 620766.

Twenge, J. M. (2017). *iGen: Why today's super-connected kids are growing up less rebellious, more tolerant, less happy--and completely unprepared for adulthood--and what that means for the rest of us*. Simon and Schuster.

Van Puyvelde, D., Coulthart, S., & Hossain, M. S. (2017). Beyond the buzzword: big data and national security decision-making. *International Affairs*, *93*(6), 1397–1416.

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32–46.

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe Report. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

Wilson, T., Brown, J., & Clark, H. (2022). Social Media Savvy: Harnessing Gen Z for Intelligence Gathering. *International Journal of Intelligence and Counterintelligence*, *35*(2), 145–160.

Yazdi, M. V. (2021). The digital revolution and the demise of democracy. *Tul. J. Tech. & Intell. Prop.*, *23*, 61.