Digital transformation on national security strategy: A bibliometric analysis

Andi Luhur Prianto[1,*], Aqmal Reza Amri[1], Goran Ilik[2]

[1]Faculty of Social and Political Sciences, Universitas Muhammadiyah Makassar, Makassar, Indonesia
[2]Faculty of Law, University "St. Kliment Ohridski", Bitola, North Macedonia

Article history
Received: 12 April 2025
Revised: 23 April 2025
Accepted: 26 April 2025

Keywords
Digital Transformation
National Security
Security Strategy

Abstract
Digital transformation has profoundly impacted numerous sectors, with national security no exception. This article undertakes a thorough analysis of how digital transformation influences strategies in national security. Employing a bibliometric approach, the study explores the proliferation of digital technologies and their implications for security policies and frameworks. The research identifies key trends, thematic developments, and emerging research fronts at the intersection of digital transformation and national security. It becomes evident that digital technologies such as artificial intelligence, blockchain, and cybersecurity measures play crucial roles in enhancing national defence capabilities and addressing contemporary security threats. These technologies offer unprecedented opportunities for efficiency and effectiveness in security operations. However, alongside these benefits come new challenges, prominently cybersecurity risks and the necessity for robust regulatory frameworks. Integrating advanced technologies into national security strategies demands vigilant management to mitigate potential vulnerabilities and safeguard sensitive information. The article concludes by offering strategic recommendations for policymakers to navigate the complexities of the digital landscape while effectively bolstering national security. These recommendations emphasise the importance of adaptive policies that foster innovation while ensuring resilience against evolving threats. Overall, this research contributes significantly to the expanding literature on digital transformation by providing insights into its profound implications for national security. It sets the stage for future studies to delve deeper into specific technological impacts and policy responses necessary to maintain a secure digital environment.

1. Introduction

The shift towards using digital technology and implementing modern information technology is a highly relevant issue and a global concern (Fitzgerald et al., 2013). This is not just a trend but a crucial necessity that affects various sectors (El Kadiri et al., 2016). Digital transformation significantly changes work processes and operations, enhancing efficiency, productivity, and competitiveness in addressing contemporary challenges (Kraus et al., 2021; Malikova et al., 2022). Digital technology can automate tasks that previously required significant time and human effort (Acemoglu & Restrepo, 2019; Wiklund, 2022). This reduces operational costs and enables more strategic and creative problem-solving (Warner & Wäger, 2019). Digital transformation refers to integrating digital technology into all areas of business and government, fundamentally changing how organisations operate (Karmous-Edwards et al., 2022; Malikova et al., 2022). Digital transformation brings significant changes across various sectors, including government, military, economy, and social life (Bertola & Teunissen, 2018; Brunetti et al., 2020; Cooper, 2019). Governments that adopt digital technology can improve the efficiency of public services, enhance transparency, and increase citizen participation in democratic processes(Lee-Geiller & Lee, 2019; Saner et al., 2020). For example, e-government allows for the provision of public services online, facilitating citizens' access, reducing corruption, and enhancing administrative efficiency (Ismail et al., 2020; Rustiarini, 2019; Valle-Cruz, 2019). Furthermore, digital transformation has also become a driving force in improving efficiency and effectiveness in various sectors, including national security (Ohkubo, 2019). The application of digital technology in national security brings significant changes to protect the nation from internal and external threats and enhance crisis management capabilities (Abd Al Ghaffar, 2024; Montasari, 2022).

Historically, national security strategies primarily focused on conventional threats such as military aggression and espionage (Cunliffe, 2016; Heath et al., 2017; Syed & Javed, 2017). However, with the advent

*Corresponding author, email: luhur@unismuh.ac.id of the digital era, the national security landscape has evolved to encompass cyber threats, digital espionage, and the use of advanced technology by state and non-state actors (Kello, 2023; Shahzad Akram, 2023). The digital transformation of national security strategies represents a fundamental shift in how countries address emerging threats (Cooper, 2019). The integration of digital technology offers significant potential to enhance capabilities, improve decision-making, and respond to new challenges (Alqadhi et al., 2023; Dwivedi et al., 2021; Kache & Seuring, 2017). However, it also introduces risks and vulnerabilities that must be carefully managed (Hanelt et al., 2021). The increased reliance on digital infrastructure in various aspects of government and defense has led countries worldwide to invest heavily in digital technology to modernize their security apparatus (Chehabeddine & Tvaronavičienė, 2020; Mori, 2019; Shackelford & Craig, 2014). Technologies such as artificial intelligence, blockchain, and advanced cybersecurity measures have become integral to national security strategies (Al-Suqri & Gillani, 2022; Dimitrov, 2020). However, the rapid pace of technological advancement necessitates continuous evaluation of how these technologies are integrated and managed (Pătrașcu, 2021).

Digital transformation and national security strategy are increasingly inseparable concepts in the modern era (Baylis & Wirtz, 2015; Mergel et al., 2019). The connection between the two becomes increasingly significant as technology evolves and cyber threats rise (Adigwe et al., 2024; Darıcılı & Çelik, 2021). Digital transformation opens opportunities to strengthen national security strategies through the use of advanced technologies such as artificial intelligence (AI), big data analytics, and the Internet of Things (IoT) (Tran-Dang & Kim, 2021). AI can detect and respond to cyber threats more effectively, while big data analytics can assist in collecting and analyzing intelligence to identify threat patterns (Montasari, 2022). IoT can enhance surveillance and control capabilities but also introduces new risks that must be carefully managed (Mahor et al., 2022). Digital transformation brings many benefits but increases risks, requiring more sophisticated and integrated security approaches (Chawla & Goyal, 2022; Doukidis et al., 2020; Zaki, 2019). Countries must be able to navigate this complexity to protect national interests and maintain security in an increasingly digital world(Fjäder, 2014; Strand, 2016). In the geopolitical context, digital transformation also influences global power dynamics (Barrinha & Renard, 2020; Bounfour, 2016; Dąbrowska et al., 2022; Gray, 2021). Countries that excel in digital technology have strategic economic and military advantages(Hanna, 2018; Lewis, 2019). Therefore, investment in digital infrastructure and the development of technological capabilities have become priorities in the national security strategies of many countries (Demchak & Dombrowski, 2014; Dunn Cavelty & Wenger, 2020; Omand, 2014). Digital transformation is not just about technology but also about preparing nations to face challenges and seize opportunities in the digital era (DeNardis, 2014; Harris, 2014; Mosco, 2017; Owen, 2015).

The digital transformation of national security strategy represents a fundamental shift in how countries address emerging threats (Carr, 2016; ElMassah & Mohieldin, 2020). Studying digital transformation and national security is crucial because it helps identify key trends and developments in this rapidly evolving field (Kraus et al., 2021). By understanding the current state of research, policymakers and practitioners can make informed decisions regarding adopting and integrating digital technology. The background of this study is rooted in the recognition that digital transformation is not merely a technological trend but a fundamental shift impacting all aspects of society, including national security. For national security, this means leveraging technologies such as artificial intelligence (AI), machine learning, big data analytics, and blockchain to enhance capabilities and respond to emerging threats (Agarwala & Chaudhary, 2021a; Zeadally et al., 2020). Adopting these technologies requires a comprehensive understanding of their potential positive and negative impacts on national security (Jagatheesaperumal et al., 2022; Radanliev, 2024). The motivation for this study stems from the critical need to improve our understanding of digital transformation in national security.

Previous studies have highlighted the relationship between information and communication technology (ICT) and national security (Smolarek & Witkowski, 2015; Yeganegi et al., 2020), albeit with limited focus on the specific impact of digital transformation on national security strategies. Existing research often adopts qualitative approaches or concentrates solely on particular case studies, resulting in an incomplete understanding of this phenomenon (El-Kalash et al., 2018; Paschal Uchenna, 2018; Yang et al., 2015). This research becomes significant within this context by providing a comprehensive bibliometric analysis to fill this knowledge gap. Prior studies have underscored the importance of adapting national security strategies to the developments in ICT (Aisenberg, 2018; Johnson, 2020; Shafqat & Masood, 2016; Tropina & Callanan, 2015). However, many of these studies still concentrate on specific aspects of digitisation, such as cyber security, electronic surveillance, or the use of technology in military conflicts. In contrast, this article delves explicitly into the holistic impacts of digital transformation on national security strategies. Comparison with previous research indicates that much of the earlier studies tend to be descriptive or qualitative in understanding the implications of digital transformation on national security. One novelty of this research lies in the bibliometric analysis approach employed to explore relevant literature. Through this technique, the authors can identify major trends, publication patterns, and collaboration networks among researchers in digital transformation and national security. This research adopts a bibliometric approach, enabling a more systematic and objective analysis of existing literature. Thus, this study not only confirms previous findings but also fills gaps in the literature by providing a deeper and methodological understanding of the relationship between digital transformation and national security strategy.

Furthermore, several previous studies have discussed digital transformation issues using a bibliometric analysis approach. In general, Hajishirzi et al. (2022) have conducted research related to the digital transformation framework using a bibliometric analysis scheme. There is also research conducted by Shi et al. (2022) which provides an overview of academic research in the field of digital transformation. Apart from that, there is also research conducted by Judijanto and Solapari (2024), which uses bibliometric analysis to explore studies in the field of privacy and data security broadly. Prabawa et al. (2024) also conducted bibliometric research related to public sector development in the era of digitalization. This research provides an overview of the development of scientific research on the theme of digitalization of the public sector in the last ten years, from 2014 to 2023. These previous studies of course intersect with the research we are discussing. However, previous studies did not specifically examine the issue of digital transformation in national security issues. Not a single study has been found that discusses the issue of digital transformation in national security aspects. So this further strengthens the novelty of this research.

The objectives and aims of this study are multifaceted. Firstly, the study aims to provide a comprehensive overview of the current research landscape on digital transformation and national security. The study uses a bibliometric approach to analyse academic literature to identify key trends, thematic developments, and emerging research areas. Secondly, the study aims to identify gaps in the existing literature and propose strategic recommendations for policymakers. The study intends to contribute to the ongoing discourse on digital transformation and national security by highlighting areas requiring further research. Thirdly, the study aims to offer actionable insights for policymakers, assisting them in navigating the complexities of digital transformation and enhancing national security. This study contributes to the ongoing discussion on how digital technology can be leveraged to strengthen national security. The significance of this work lies in its potential to inform and shape national security strategies in the forthcoming digital era. The strengths of this research include providing a detailed analysis of current trends and challenges, offering actionable insights for policymakers, and laying the groundwork for future studies in this domain. Ultimately, the study aims to bridge the gap between technological advancements and national security imperatives, ensuring that digital transformation acts as a catalyst for enhancing national defense capabilities.

2. Literature Review

Digital transformation refers to integrating digital technologies into all aspects of an organization, fundamentally altering its operations and delivering value to stakeholders (Fedotova et al., 2019; Johnson, 2020). In the context of national security, this transformation encompasses a range of technologies and practices, from cyber defence and intelligence gathering to data analysis and surveillance systems (Akhgar et al., 2015; Denning, 2014; Gupta & Pathak, 2022). One of the main drivers of digital transformation in national security is the evolving nature of threats in the digital age (Cunliffe, 2016; Roy, 2006). Traditional security paradigms are no longer sufficient to address the complex and dynamic challenges posed by cyberattacks, disinformation campaigns, and other forms of hybrid warfare (J. Brown, 2018; Tsaruk & Korniiets, 2020; Weissmann et al., 2021). Consequently, governments and security agencies increasingly use digital technologies to enhance their capabilities and resilience against emerging threats (Argyroudis et al., 2022; Brass & Sowell, 2021; Linkov et al., 2018). One area where digital transformation is reshaping national security strategies is in the field of cyber defence (Galinec et al., 2017; Senol & Karacuha, 2020). With the rise of cyberattacks targeting critical infrastructure, government networks, and private companies, robust cybersecurity measures are growing and are needed to protect against potential threats (Lehto, 2022; Rudner, 2013). This has led to the development of advanced security solutions, such as intrusion detection systems, threat intelligence platforms, and encryption technologies, to safeguard sensitive information and infrastructure from malicious actors (Preuveneers et al., 2020; Saxena & Gayathri, 2021).

Moreover, digital transformation is revolutionizing national security agencies' intelligence gathering and analysis processes (Kadtke & Wells, 2014; Lowenthal, 2022). By leveraging big data analytics, machine learning algorithms, and artificial intelligence tools, agencies can sift through vast amounts of information to identify patterns, detect anomalies, and predict future threats more accurately and efficiently (Montasari, 2023; Rubin et al., 2014). This enables proactive decision-making and strategic planning, enhancing the overall effectiveness of national security operations (Alguliyev et al., 2020; Bondarchuk P, 2021; Lee, 2020). Furthermore, digital transformation facilitates greater collaboration and information sharing among the various stakeholders involved in national security efforts (Kouroubali & Katehakis, 2019; Saranov, 2019). Government agencies, law enforcement bodies, and international partners can exchange intelligence, coordinate responses, and enhance situational awareness in real time through connected networks and information-sharing platforms (Jenkins et al., 2014; Pfeifer, 2012). This collaborative approach is crucial for addressing cross-border threats, such as terrorism, organized crime, and the proliferation of weapons of mass destruction, which require coordinated and comprehensive responses from the international community (Casino et al., 2022; Legrand & Leuprecht, 2021). However, along with the opportunities presented by digital transformation, some significant challenges and risks need to be addressed (Anunciação et al., 2021). One major concern is the growing threat of cyberattacks and information warfare, which can disrupt critical infrastructure, undermine public trust, and compromise national security objectives(Favoretto et al., 2022; Kormych et al., 2024). Additionally, the rapid pace of technological innovation and adoption introduces new vulnerabilities and complexities that can be exploited by malicious actors, necessitating continuous adaptation and investment in cybersecurity capabilities (An, 2022; Anunciação et al., 2021; Shah, 2021; Sobb et al., 2020).

Research on the impact of digital transformation on national security strategies highlights the crucial role of digital technologies in transforming how governments and security agencies operate to address modern threats (Bannykh & Kostina, 2021; Jansen et al., 2023; Roberts & Schmid, 2022). These studies emphasize that the evolving threats in the digital age (Nalbantoğlu, 2022; Zhang et al., 2023), such as cyberattacks (Makarychev & Wishnick, 2022; Masyhar & Emovwodo, 2023), disinformation campaigns (Soesanto, 2023), and hybrid warfare (Upadhyay, 2023), demand a shift from traditional security paradigms toward more sophisticated and dynamic approaches. The research also acknowledges the significant challenges and risks accompanying digital transformation (Douzet & Gery, 2021; Mutanda, 2024; Pylypenko et al., 2022). The evolving cyber threats and information warfare can disrupt critical infrastructure and erode public trust (Bareis & Katzenbach, 2022; Douzet & Gery, 2021; Hermeto, 2021). Additionally, the rapid pace of technological innovation introduces new vulnerabilities and complexities that can be exploited by malicious actors, requiring ongoing adaptation and investment in cybersecurity capabilities(Ifeanyi-Ajufo, 2023). These studies indicate that while digital transformation offers substantial opportunities to strengthen national security strategies, a careful and holistic approach is necessary to address emerging challenges and mitigate associated risks. The research literature taxonomy can be seen in Table 1.

Table 1. Research literature taxonomy.

Title	Insights	Summarized Abstract	Results
The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks	The paper examines how terrorist organizations, particularly ISIS, adapt to cyber technologies, impacting global security and society, and recommends comprehensive measures to counter these threats.	This study analyzes ISIS's use of cyberspace for recruitment, propaganda, and cyberattacks, highlighting the global reach of cyberterrorism and calling for enhanced digital literacy, international cooperation, and stringent regulations.	ISIS has expanded its global influence through digital platforms, with increasingly sophisticated cyberattacks causing significant socio-economic impacts, necessitating a multifaceted approach, enhanced digital literacy, international cooperation, and stringent regulations on advanced technologies.
Fortifying the Global Data Fortress: A Multidimensional Examination of Cyber Security Indexes and Data Protection Measures across 193 Nations	The article explores global cybersecurity by analyzing key indexes and provides insights for enhancing data protection and fostering international collaboration.	This study examines global cybersecurity using four indexes across 193 countries, uncovering correlations, regional disparities, and trends to inform policymakers and stakeholders on enhancing data protection and fostering international cooperation.	The study identifies potential correlations, regional disparities, and emerging trends in cybersecurity, providing insights to enhance data protection, promote cross-border collaboration, and build a resilient global digital ecosystem.

Title	Insights	Summarized Abstract	Results
Cyber Security Threats and Countermeasures in the Digital Age	The article explores the evolving cyber threat landscape in the digital age and provides actionable countermeasures to enhance cybersecurity for individuals, businesses, and governments.	This study analyzes the cyber threat environment, detailing threats like malware and phishing, and examines advanced tactics used by cybercriminals. Emphasizing a multi-layered security approach and the importance of collaboration among individuals, businesses, and governments, it offers strategies to mitigate risks and promote cybersecurity awareness in the digital age.	The study identifies a range of cyber threats and evolving tactics cybercriminals use, highlighting the increasing risks from advanced technologies like IoT and AI. It underscores the need for a multi-layered security strategy and collaborative efforts to effectively counter these threats and foster a culture of cybersecurity awareness.
State Defense: Challenges Towards Digitalization	The article discusses Indonesia's national resilience, emphasizing the importance of state defense and citizen participation in maintaining unity and integrity in the digital age.	This study explores Indonesia's national resilience and state defense, highlighting the nation's ability to face internal and external threats to ensure unity and integrity. It emphasizes the role of citizens, inspired by their love for Indonesia, in defending the country based on Pancasila and the 1945 Constitution and underscores the legal framework governing state defense participation.	Indonesia's national resilience is vital for maintaining unity and integrity, with state defense relying on citizens' commitment to serve and sacrifice, governed by laws, to ensure effective participation in overcoming digital-era challenges.
Terrorist crimes in the era of Digitalization: forms of activity and measures for counteraction	The article examines how digitalization has transformed terrorist activities and proposes strategies for countering these crimes effectively.	This study aims to develop recommendations for countering terrorist crimes in the digital space, using various scientific methods to analyze how digital technologies have intensified terrorism and altered crime mechanisms. It concludes that an effective counter-strategy requires a clear regulatory framework and highlights the need to adjust criminalization to address the use of digital technologies in terrorism.	The study identifies the increased intensity of terrorism due to digital technologies, emphasizing the need for a strategic and regulatory framework to counteract terrorist activities such as propaganda, recruitment, training, and funding conducted through digital means.
Digital Transformation and Its Impact on the Application of Cyber Security in the Ministry Of Interior and National Security in Palestine	The article explores how digital transformation impacts cybersecurity practices in the Palestinian Ministry of Interior and National Security, providing recommendations for improvement	This study investigates the correlation between digital transformation and cybersecurity effectiveness in the Palestinian Ministry of Interior and National Security, emphasizing the need for budget allocation, staffing adequacy, and enhanced threat detection capabilities.	The study identifies a strong correlation between digital transformation dimensions and cybersecurity application, with specific factors like organizational structure and technical infrastructure significantly influencing cybersecurity effectiveness.
The Reality of Digital Transformation in the Palestinian Ministry of Interior and National Security	The article evaluates digital transformation in the Palestinian Ministry of Interior and National Security, offering recommendations for enhancement.	This study assesses digital transformation in the Ministry through employee perspectives, finding significant presence and approval of various dimensions.	Findings show high approval for digital transformation dimensions, including senior management support, strategic directions, technical infrastructure, human resources, coordination, data privacy, and organizational structure, with recommendations emphasizing budget allocation and innovation in service provision.

Title	Insights	Summarized Abstract	Results
Cybersecurity Technologies Essential in the Digital Transformation Era	The article highlights the increasing security risks brought by digital transformation and emphasizes the urgent need for cybersecurity technologies to mitigate these risks.	In the digital transformation era, new technologies like IoT and OT are creating advanced economic activities but also increasing security risks. This paper outlines the need for enhanced security technologies across IT, IoT, and OT domains to address evolving threats and protect data use in society.	The study emphasizes the importance of expanding threat monitoring targets to include endpoint and backbone networks, developing breakthrough countermeasure functions for IoT and OT, and leveraging cryptographic techniques to safely handle privacy and confidential information in society's evolving data environment.
The digital transformation of intelligence analysis	The article explores how digital transformation can effectively enhance intelligence analysis to combat organized crime.	This paper examines the potential of digital transformation in intelligence analysis, emphasizing the importance of data, information technologies, and human development in simplifying complex processes.	The study highlights the impact of digital phenomena on human activity and the competitive advantage of effective digital transformation, advocating for an activity-based intelligence model to address challenges posed by organized crime efficiently. It serves as a guide for law enforcement professionals, emphasizing the significance of organizational innovation and the emerging applications-based culture in simplifying expert-based processes in intelligence analysis.
Digital transformation meets national development requirements	The article explores how digital transformation is reshaping socio-economic development in Vietnam, highlighting challenges and opportunities.	In the era of the fourth industrial revolution, digital transformation emerges as a key driver of socio-economic progress in Vietnam, prompting the need for refined policies to meet national development requirements.	While digital transformation holds potential for improving quality of life and fostering development, it currently falls short of meeting Vietnam's socio-economic needs, necessitating enhanced policies and strategies for rapid advancement.
Cybercrime in the Age of Digital Transformation, Rising Nationalism and the Demise of Global Governance	Rising cybercrime, driven by nationalistic cyber policies, undermines global governance and poses challenges for law enforcement in the digital transformation era.	In the Fourth Industrial Revolution, cybercrime escalates due to nationalistic cyber policies, hindering global governance and trust in public-private partnerships, and complicating law enforcement efforts.	Cybercrime's surge, fueled by nationalistic cyber policies, disrupts global governance, erodes trust in partnerships, and burdens law enforcement with insufficient legal frameworks.
How the Digital Transformation Changed Geopolitics	The article explores how digital transformation has reshaped geopolitics, leading to significant disruptions and challenges.	Technological advancements in the late 2000s transformed data into a valuable asset, altering economic dynamics and incentivizing strategic policies. These changes reconfigured geopolitical rivalries, creating vulnerabilities to information warfare and fueling social and political conflicts.	Digital transformation has shifted great power rivalry, created vulnerabilities to information warfare, and fueled social and political conflicts, despite US leadership in technological innovation, highlighting the need to adapt to evolving technological and economic conditions.
Digital Transformation Security Challenges	The article stresses the importance of integrating security into digital transformation strategies to mitigate data breaches and security risks.	Developing a digital strategy without security considerations poses serious risks of data breaches in the digital age. Despite countermeasures, security remains a major concern in digital transformation, leading to various security issues across organizations. This study aims to identify barriers to digital innovation by analyzing common elements impacting security through literature review and case study.	The study highlights barriers to digital innovation, underscoring the need to address security concerns in digital transformation strategies for successful implementation and risk mitigation.

3. Method

This study employs a bibliometric analysis approach to explore the impact of digital transformation on national security strategy. Bibliometric analysis is a method used to assess and analyze scientific literature through the statistical measurement of articles, citations, and other publication data. This approach enables researchers to identify research trends, collaboration patterns, and academic influence in a particular field. The data used in this study were obtained from major scientific databases such as Dimensions AI, Scopus, and Google Scholar. The keywords used in the search included "digital transformation," "national security," "digital strategy," and "security policy." This search covered the period from 2020 to 2024 to ensure comprehensive coverage of relevant literature. This study applies strict inclusion and exclusion criteria to ensure that only relevant and high-quality literature is analyzed. The inclusion criteria include articles published in peer-reviewed journals, written in English, and directly related to the topic of digital transformation and national security. The exclusion criteria include articles that are not available in full text, not relevant to the main topic, or published in languages other than English. The study selection process follows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flow diagram, which consists of four stages: identification, screening, eligibility, and inclusion. The PRISMA diagram used in this study is as follows (Figure 1):

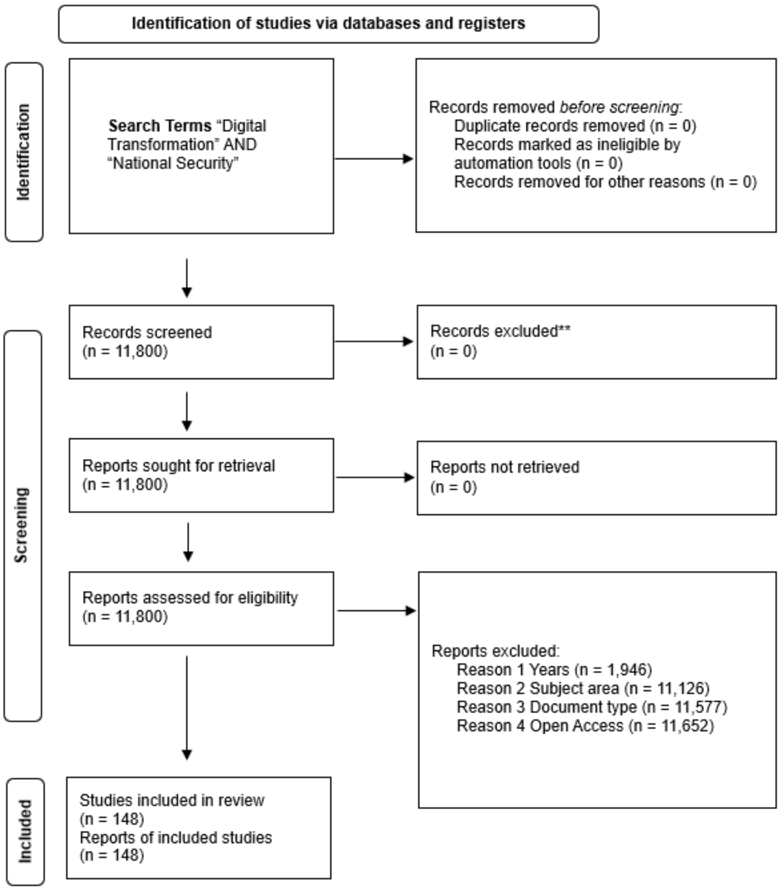

Identification of studies via databases and registers
Identification
Search Terms "Digital Transformation" AND "National Security"
Records removed *before screening*:
Duplicate records removed (n = 0)
Records marked as ineligible by automation tools (n = 0)
Records removed for other reasons (n = 0)
Screening
Records screened (n = 11,800)
Records excluded** (n = 0)
Reports sought for retrieval (n = 11,800)
Reports not retrieved (n = 0)
Reports assessed for eligibility (n = 11,800)
Reports excluded:
Reason 1 Years (n = 1,946)
Reason 2 Subject area (n = 11,126)
Reason 3 Document type (n = 11,577)
Reason 4 Open Access (n = 11,652)
Included
Studies included in review (n = 148)
Reports of included studies (n = 148)

Figure 1. Prisma flow diagram – author.

Identification: At this stage, a total of 11,800 articles were identified through database searches.
Screening:
R1: Of the 11,800 articles, 1,946 were filtered based on the publication year of the last five years.
R2: Of the 11,800 articles, 11,126 were filtered based on the subject area, specifically Social Science.
R3: Of the 11,800 articles, 11,577 were filtered based on the document type, specifically articles.
R4: Of the 11,800 articles, 11,652 were filtered based on Open Access availability.
Included: A total of 148 articles were assessed for eligibility by examining the full text to ensure they met the inclusion criteria. Finally, 148 articles were selected for further analysis. The 148 articles were the result of filtering using the Prisma model. The articles that were filtered using indicators R1, R2, R3, and R4 were finally re-evaluated to check their suitability and relevance regarding the research theme raised. This was done to obtain high quality articles which will later be analyzed further in this research.

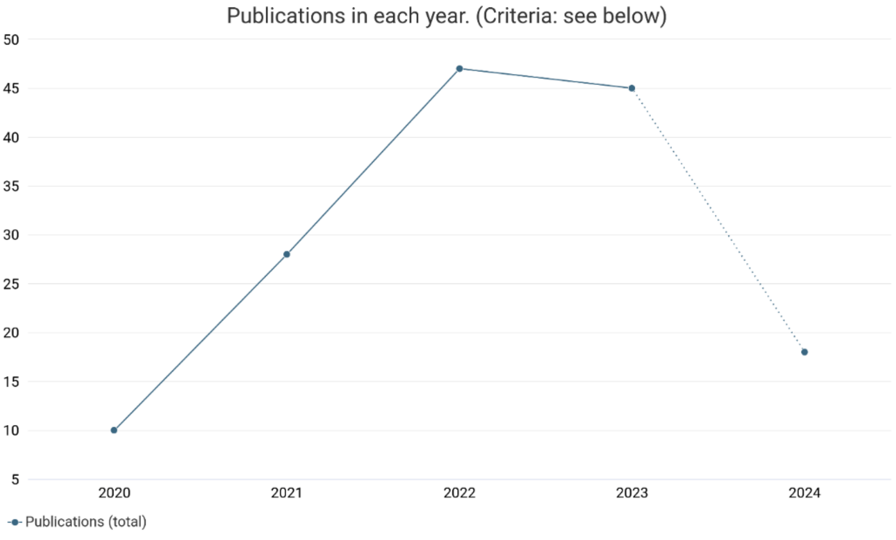
Following the included stage, bibliometric analysis was conducted using software such as VOSviewer. This analysis included the evaluation of publication frequency, author collaboration networks, keyword mapping, and citation analysis. Additionally, content analysis was performed to identify major themes and research trends within the selected literature. Cross-checking among researchers was performed during the study selection and data analysis stages to ensure the validity and reliability of the research findings. Moreover, data triangulation methods were used to compare results from multiple databases and analysis software to reduce bias and enhance the accuracy of the findings. By employing this approach, the study aims to provide a deep understanding of how digital transformation affects national security strategy and identify critical areas requiring further attention from researchers and policymakers.

4. Result and Discussion

4.1. Research Trend: Digital Transformation and National Security Strategy

4.1.1. Trend Publication by Year

Figure 2 depicts the trend in the number of research publications over the past five years, from 2020 to 2024, that examine the topic of “Digital Transformation” and its relation to “National Security.” The data illustrates how academic attention to this issue has evolved and shifted throughout this period. In 2020, the recorded number of publications was approximately 10. This reflects the initial recognition of the importance of digital transformation in the context of national security. The year 2020 can be seen as a starting point where researchers began to seriously explore the relationship between digital transformation and national security, with a relatively low but significant number of publications laying the foundation. Entering 2021, there was a considerable increase in the number of publications, reaching around 30. This rise indicates heightened awareness and interest among academics and researchers in this topic. The accelerated pace of digital transformation across various sectors, especially due to the impact of the COVID-19 pandemic (Brummer & Ueno, 2024; Hai et al., 2021), further spurred research into how digitalization affects aspects of national security. During this year, issues such as cybersecurity, data protection and critical infrastructure received more attention due to the increasing reliance on digital technologies (Hurel, 2022; Kuzior et al., 2022; Mishra & Gochhait, 2024; Möller, 2023a, 2023b; Mongeau & Hajdasinski, 2021).



Source: https://app.dimensions.ai
Exported: June 08, 2024
Criteria: "Digital Transformation" AND " National Security" in full data; Publication Year is 2024 or 2023 or 2022 or 2021 or 2020; Fields of Research (ANZSRC 2020) is 4408 Political Science; Publication Type is Article; Open Access is All OA.

© 2024 Digital Science and Research Solutions Inc. All rights reserved. Non-commercial redistribution / external re-use of this work is permitted subject to appropriate acknowledgement. This work is sourced from Dimensions® at www.dimensions.ai.

Figure 2. Publication of documents by year – dimension AI.

The positive trend continued in 2022, with the number of publications rising to around 45. This consistent increase signifies the peak of academic interest in this topic within the studied period. This year can be considered a period where the topic of digital transformation and national security became more mature in academic literature. Many studies began to focus more on specific aspects such as the use of artificial intelligence in national security, the impact of blockchain technology, and the development of policies and regulations related to new technologies (Ahad et al., 2023; Alareeni & Elgedawy, 2023; Banafa, 2020; Bharat Vagadia, 2017; Möller, 2023a). The rising number of publications also indicates that more researchers are engaging in exploring various dimensions of digital transformation in the context of national security. In 2023, the number of publications slightly decreased but remained around 45, indicating stabilization in the amount of research being conducted. Despite the slight decline, this stability signifies that interest in this topic remains high and continues to be a significant area for research. Many researchers in this year observed a consolidation of previous findings and began exploring the practical implications of various technological innovations in the field of national security (Moussa & Tarek, 2023; Oling et al., 2022; Pătraşcu, 2021; Rubin et al., 2014; Yao & Fu, 2023). The stability in the number of publications may also suggest that researchers are delving deeper, not merely increasing the number of studies but also enhancing the quality and depth of their analyses.

However, in 2024, the data shows a sharp decline in the number of publications, returning to around 10. This significant decrease reflects several factors. One factor is that the data for 2024 might not be fully compiled as it was collected at the beginning of the year. Academic publications often require time from the research stage to publication, so there may be several publications not yet recorded. Another contributing factor is a shift in research focus or changes in funding and policy priorities affecting the number of studies conducted. This decline may also indicate that researchers are beginning to shift to other topics or more specific sub-topics within the domain of digital transformation and national security. Meanwhile, it is possible that this topic has been sufficiently explored in recent years, resulting in a decrease in new publications as existing research has addressed many initial questions. Nevertheless, it is essential to consider that this trend could change again with technological advancements and shifts in the geopolitical and global security context.

4.1.2. Trend Publication by Subject Area

Figure 3 shows the distribution of research documents by subject area focused on the topic of digital transformation and its relation to national security issues. This chart provides insight into how academic attention to this topic is spread across various disciplines. The most notable feature in this chart is the dominance of "Social Sciences," which accounts for 35.4% of the total documents. This dominance indicates that digital transformation and national security are highly relevant in the context of social and policy studies. Social sciences encompass various fields such as sociology, political science, anthropology, and media studies, all of which play a crucial role in understanding the social impacts of digitalization. Research in social sciences explores how digital transformation affects power relations, social behaviour , security policies, and social dynamics (Dear, 2022; Ilyina, 2022; Kormych et al., 2024). This also reflects how national security and digitalization issues have become significant topics in public policy and administration studies, considering the broad impact of digital technology on society (Matos et al., 2020; Milakovich, 2021; Rackwitz et al., 2021). Next, "Computer Science" ranks second with 16.4% of the total documents. The prominence of computer science in this research indicates the importance of technical aspects in understanding digital transformation and national security issues. Research in this field includes cybersecurity, algorithm and encryption development, big data analysis, and artificial intelligence (Khan et al., 2020; Radanliev, 2024). Computer science plays a vital role in developing technologies that can enhance national security through innovative digital solutions and in identifying and addressing increasingly complex cyber threats.

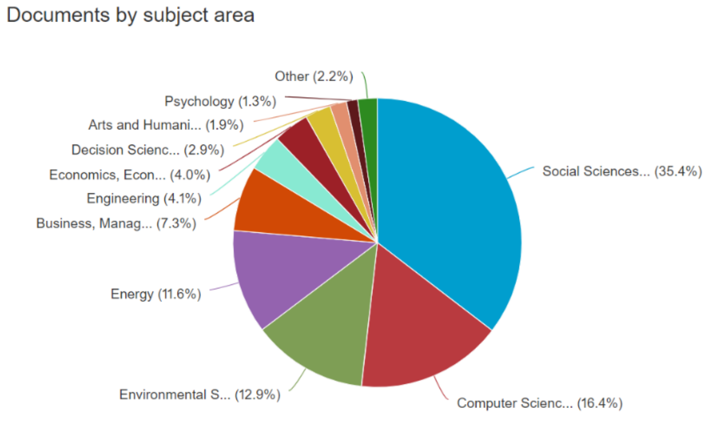


Figure 3. Publication of documents by subject area-Scopus.

"Environmental Science" also holds a significant portion with 12.9%. This indicates considerable attention to how digital transformation can impact and be impacted by environmental issues. For instance, digital technologies can be used for environmental monitoring, disaster mitigation, and efficient resource management (Ren et al., 2023; Sun, 2024; Yao & Fu, 2023; Yu et al., 2023). Additionally, there is concern about the environmental impact of digital technology use, such as the carbon footprint of data centers and electronic devices (Wei & Wang, 2021; Xin et al., 2022; Xu et al., 2023). The relationship between national security and the environment is becoming increasingly important, given that climate change and natural disasters can affect national and international stability. The "Energy" field accounts for 11.6% of the documents, reflecting how digital transformation affects the energy sector and its relation to national security (Chygryn et al., 2022; Rajavuori & Huhta, 2020). Research in this field includes using digital technology to improve energy efficiency, manage smart grids, and protect critical energy infrastructure from cyber threats(Kapitonov et al., 2020; Thanh et al., 2023). Digital transformation in the energy sector also involves the use of big data and analytics to predict and manage energy needs and reduce reliance on unstable energy sources (Akberdina & Osmonova, 2021; Chwiłkowska-Kubala et al., 2023; Maroufkhani et al., 2022; Nazari & Musilek, 2023). "Business and Management" occupies 7.3% of the total documents, highlighting the relevance of this topic in the economic and corporate strategy context. Research in this area focuses on how companies can adopt digital technologies to enhance security and operational efficiency and how digital risk management can be applied in the context of national security (Chygryn et al., 2022; Mishra & Gochhait, 2024; Shakarishvili & Tbilisi, 2024). This also includes studies on the role of technology companies in providing digital security solutions and how they collaborate with governments in facing cyber threats (Bogoyavlenska et al., 2023; Poliakova et al., 2024; Popkova, 2022; Ştefan, 2022). The "Engineering" discipline contributes 4.1% of the total documents. This reflects the focus on engineering and technological aspects that support digital transformation and national security. Engineering research includes developing security hardware and software, information technology infrastructure, and advanced surveillance and control systems (Grisales Rendón, 2022; Su & Flew, 2020). Engineering aspects are crucial in building and maintaining secure and reliable technological infrastructure (Mamediieva & Moynihan, 2023; Mishra & Gochhait, 2024; Tuskov et al., 2023). "Economics," with 4.0% of the total documents, shows how digital transformation and national security influence and are influenced by economic dynamics. Economic research involves cost-benefit analysis of security technology implementation, cyberattacks' economic impact, and economic policy's role in supporting safe digital transformation(Kravchenko, 2024; Paunov & Guellec, 2024; Singh & Singh, 2022; Zhong et al., 2022).

"Decision Sciences" and "Arts and Humanities" each contribute 2.9% and 1.9% of the documents, respectively. Decision sciences include data-driven analysis and decision-making for security strategies, while arts and humanities cover cultural and ethical studies of digitalization and security(Abbu et al., 2024; Mao & Shi-Kupfer, 2021; Weber-Lewerenz, 2022). Both fields demonstrate a multidisciplinary approach to understanding the complexity of digital transformation. "Psychology," with 1.3% of the total documents, shows how human factors and behaviour influence and are influenced by digital transformation in the context of national security. Psychological research includes studies on risk perception, compliance with security protocols, and the psychological impact of cyber threats (Adisa & Mordi, 2022; Akande, 2023; Nguyen et al., 2020; Tomczyk et al., 2023). Finally, the "Other" category contributes 2.2% of the total documents, encompassing various other fields that contribute to a holistic understanding of digital transformation and national security. This reflects the broad scope of this topic and the importance of an interdisciplinary research approach. The distribution of documents by subject area shows that the topic of digital transformation and national security encompasses various disciplines, with the main dominance in social sciences and computer science. This reflects the complexity and multidimensionality of this topic, as well as the importance of cross-disciplinary collaboration in developing a comprehensive understanding and effective solutions to the challenges faced. Digital transformation brings significant changes that affect almost all aspects of life, and national security is one of the most critical areas in this context. Research spanning various fields of science shows the vastness and depth of this issue and the need for a holistic and integrated approach to addressing the challenges and leveraging the opportunities presented by the digital age.

4.1.3. Trend Publication by Subject Area

Figure 4 illustrates the distribution of research documents by country or territory focused on the topic of digital transformation and its relationship to national security issues. The data in the chart reveals which countries are leading in academic output on this subject, offering insights into regional focuses and contributions to the field. China stands out prominently with the highest number of research documents, significantly surpassing other countries. This dominance highlights China's extensive investment and interest in the intersection of digital transformation and national security. China's rapid technological advancements and strategic initiatives, such as its emphasis on cybersecurity and the development of digital infrastructure, underscore its focus on harnessing digital transformation to bolster national security. The substantial volume of research from China reflects its prioritization of understanding and addressing the implications of digital technologies for national security. China's dominance of publication trends by region is proof of the Chinese government's seriousness in responding to national security threats in the digital era(Lindsay, 2014; Lindsay et al., 2015; Qiang, 2019). The seriousness of the Chinese government can be seen from the government's strong and coordinated policies in supporting the digital transformation process as part of the national development strategy (He et al., 2020; Y. Liu et al., 2018; Peng, 2022). Initiatives such as Made in China 2025 and the Smart City program demonstrate China's commitment to becoming a global leader in digital technology and innovation (Agarwala & Chaudhary, 2021b; Parasol, 2018; Riva Sanseverino et al., 2018; Wübbeke et al., 2016; Zenglein & Holzmann, 2019). Additionally, national security is a top priority for China, with a focus on cyber security and the development of advanced military technology(Allen, 2019; Caplan, 2013; Sayler, 2020). The articles analyzed in this context explain several research focuses covering various aspects ranging from public policy, and information technology, to social studies regarding the impact of digitalization.

Following China, the United Kingdom is the second-highest contributor in terms of research documents. The UK's strong academic tradition and its active involvement in global cybersecurity discussions contribute to its substantial research output. The UK’s focus on digital transformation and national security encompasses various aspects, including policy development, technological innovations, and international collaborations. The presence of leading research institutions and think tanks further supports the country's significant contribution to this field. The UK has a highly developed technology sector and is the center of digital innovation in Europe(Bilozubenko et al., 2022; Dommett, 2020; Humm et al., 2021). UK government policies that support digitalization, such as the UK Digital Strategy, demonstrate the country's commitment to digital transformation (Margetts & Dunleavy, 2013; Philip et al., 2017). In addition, the UK also has a strong focus on national and cyber security, considering cyber threats are increasingly increasing and complex (Carr, 2016; Guitton, 2013; Stoddart, 2016; Tatar et al., 2014). UK studies cover technical and policy aspects, as well as the social impacts of digitalization. The varied focus of these articles is because the UK needs to maintain a competitive advantage in technology and security to protect critical infrastructure and ensure national stability.

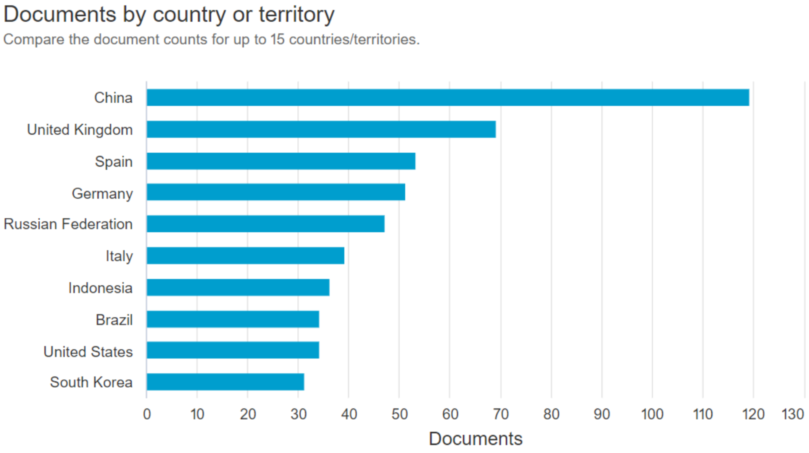


Figure 4. Publication of documents by country or territory – Scopus.

Spain ranks third, indicating a robust engagement with digital transformation and national security research. Spain's involvement in European Union initiatives and its focus on enhancing digital resilience and cybersecurity are reflected in its academic contributions. The country's emphasis on integrating digital technologies into various sectors, along with its commitment to addressing security challenges, drives its active research efforts. One of the factors why Spain ranks third is the increase in the amount of government and private investment in the digital technology and cyber security sectors(Kemp et al., 2020; Sabillon et al., 2016; Shafqat & Masood, 2016). In general, stakeholders in Spain view digitalization as key to improving government efficiency and security, as well as a tool to combat cyber threats and maintain social stability (Luiijf et al., 2013; Solar, 2020). Initiatives such as the Plan Nacional de Territorios Inteligentes demonstrate Spain's commitment to adopting digital technologies in various sectors, including national security. Research in Spain spans a wide range of disciplines, from computer science to social studies, reflecting a multidisciplinary approach to digital transformation and national security.

Germany follows closely behind Spain, showcasing its commitment to advancing research in digital transformation and national security. As a leading technological and industrial nation, Germany places a strong emphasis on developing secure digital infrastructures and innovative technologies. German research institutions and universities play a pivotal role in exploring the implications of digital transformation on national security, contributing valuable insights and solutions. The Russian Federation also makes a significant contribution to this research area, reflecting its strategic interest in cybersecurity and digital transformation. Russia's focus on protecting its digital assets and infrastructure is evident in its academic output. The country's investment in understanding the impact of digital technologies on national security is driven by its geopolitical considerations and the need to safeguard its technological advancements.

Italy's position in the middle of the chart demonstrates its active engagement in this research domain. Italy's academic contributions reflect its efforts to address the challenges and opportunities presented by digital transformation. The country's focus on developing secure digital ecosystems and enhancing cybersecurity capabilities is evident in its research output. Indonesia, Brazil, and the United States each contribute a comparable number of research documents, highlighting their respective interests in digital transformation and national security. Indonesia's academic contributions are driven by its rapidly growing digital economy and the need to ensure cybersecurity. Indonesia occupies a significant position in the number of research documents, which reflects its commitment to digital transformation. The Indonesian government has launched various initiatives to encourage the adoption of digital technology and improve cyber security, such as the National Movement of 1000 Digital Startups and the Indonesia 4.0 program (Enggarratri, 2021; Fatimah et al., 2020; Hidayatno et al., 2019; Maryanti et al., 2020). Research in Indonesia spans a wide range of disciplines, from computer science to social studies, reflecting a multidisciplinary approach to digital transformation and national security. The diverse research focuses in Indonesia are driven by the view that digitalization is the key to economic growth and increasing government efficiency, as well as a tool to combat cyber threats and maintain social stability.

Brazil's research reflects its focus on integrating digital technologies into various sectors while addressing security concerns. The United States, despite its technological leadership, shows a moderate level of research output in this specific dataset, which may be due to the diverse range of topics covered by its extensive research community. South Korea rounds out the list, showcasing its strong emphasis on digital transformation and national security. South Korea's advanced technological infrastructure and its proactive approach to cybersecurity contribute to its significant academic output. The country's focus on leveraging digital technologies to enhance national security is reflected in its research contributions. The distribution of research documents by country or territory reveals the global interest and varied regional focuses on digital transformation and national security. This diverse academic engagement underscores the need for international collaboration and knowledge sharing to effectively navigate the challenges and opportunities presented by the digital age.

4.2. Network Analysis Related to Digital Transformation on National Security Strategy

4.2.1. Network Visualization

Figure 5 is a network visualization generated by VOSviewer software. This visualization depicts the interconnections and relationships between various concepts related to digital transformation and national security issues. The network offers insights into how these topics are interrelated and organized based on their frequency of occurrence in academic literature. In this visualization, several main theme clusters can be identified based on different colors. Each cluster represents closely related research areas, identified by VOSviewer through co-word analysis. These theme clusters reflect the primary focuses of the existing literature and how these topics interact within the context of digital transformation and national security. The green theme cluster, which includes terms such as “national security,” “society,” “war,” and “crisis,” indicates a strong focus on the social and security aspects of digital transformation. The term “national security” is at the center of this cluster, suggesting that much research is concentrated on the impact of digital transformation on national security. Topics such as “society” and “war” imply that digital transformation affects physical security, social structures, and conflicts. The connection with “crisis” highlights how digital technology can exacerbate or manage emergencies and crises.

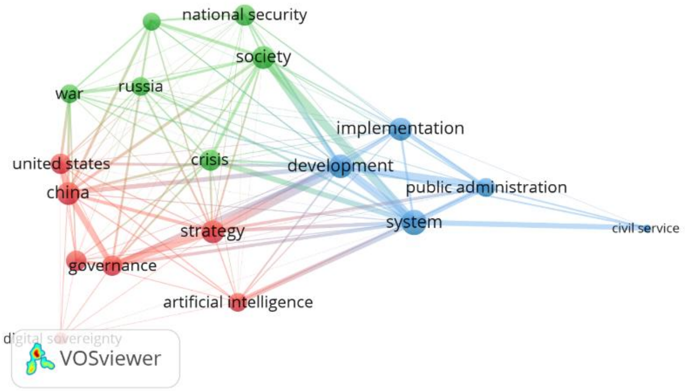


Figure 5. Network visualization of research – Vosviewer.

The red theme cluster encompasses terms such as “United States,” “China,” “strategy,” “governance,” and “artificial intelligence.” This cluster shows a geographical and strategic focus in the literature. Countries like the United States and China emerge as key players in digital transformation and national security discussions. The emphasis on “strategy” and “governance” indicates how these countries develop policies and strategies to manage digital transformation. The term “artificial intelligence” signifies that this technology is critical to digital strategies and national security policies. Furthermore, the red cluster highlights the importance of effective governance and technological development, especially in the context of relations between the United States and China. The competition between these two countries covers various aspects, from economic to military, and from politics to technology (Gilli & Gilli, 2018; Gulley et al., 2018; Zhao, 2019). The competition between the United States and China is one of the most significant global dynamics (Brooks & Wohlforth, 2015; Yeung, 2013). The two compete for dominance in a variety of fields, including technology, economics, and military (Kahler, 2013). This influences their domestic and international policies, as well as relations with other countries. Good governance is key to facing global challenges, including the economic crisis, climate change and technological developments (I. Brown & Marsden, 2023; Geels, 2013). Effective governance allows countries to better manage their resources, respond quickly to crises, and exploit technological opportunities for development. AI is one of the most influential technologies today (Dwivedi et al., 2021; Makridakis, 2017). The development and application of AI has far-reaching implications, from economics to security (Kuziemski & Misuraca, 2020; Manheim & Kaplan, 2019; Taeihagh, 2021). AI can be used to improve governance efficiency and effectiveness, but it also raises new challenges, such as data privacy, cyber security and social inequality (Makhlooqa & Mubarakb, 2024; Saura et al., 2022).

The blue theme cluster includes terms such as “implementation,” “development,” “system,” “public administration,” and “civil service.” This cluster focuses on the technical and administrative aspects of digital transformation. “Implementation” and “development” denote developing and deploying digital technologies within the context of national security. “System” and “public administration” indicate a focus on technological infrastructure and public administration management necessary to support digital transformation. “Civil service” shows how civil servants and government structures adapt to technological changes. The blue cluster focuses on aspects of public administration and systems that support policy development and implementation. This shows the importance of effective structures and processes in supporting government functions and public services. Public administration is the backbone of effective government (Bryson & George, 2020; Mayntz, 2017). It covers a wide range of functions, from human resources management to public financial management (Liu & Yuan, 2015; Osei-Kojo, 2017). Efficiency and transparency in public administration are essential to building public trust and ensuring quality services (Hartanto et al., 2021; Kettl, 2015). Good systems are the foundation for effective public administration (Asmorowati et al., 2019; Keping, 2018). This includes the physical infrastructure, information technology, and operational procedures that enable the government to run smoothly and be responsive to the needs of the community. Policy development and implementation are interrelated processes. Policy development requires in-depth analysis and strategic planning, while implementation requires effective coordination and ongoing monitoring to ensure desired results are achieved (Retnandari, 2022).

The relationships among these theme clusters demonstrate that digital transformation and national security require a multidisciplinary approach. For instance, the green cluster, focusing on national security and social impacts, connects with the red cluster, which focuses on strategy and policy through terms like "crisis" and "strategy." This indicates that crisis situations and the need for appropriate strategies are bridges between digital transformation's social and policy aspects. The red cluster also connects with the blue cluster through terms like "development" and "implementation." This shows that the strategies and policies developed by major countries such as the United States and China must be implemented and developed within technological and public administrative systems. This reflects the need to integrate strategic policies with technical and administrative implementation to achieve effective national security in the digital era. Additionally, the term "artificial intelligence" in the red cluster indicates that this technology is a key component linking strategic policies with technical implementation. The use of artificial intelligence in digital strategies and national security reflects a growing trend in both literature and practice. Artificial intelligence is used not only for data analysis and decision-making but also to enhance cybersecurity capabilities and respond to digital threats in real-time. On the other hand, the relationship between the terms "national security" and "society" in the green cluster shows that national security cannot be separated from its impact on society. Digital transformation changes how society interacts, works, and lives, significantly impacting national security. Research in this cluster focuses on how national security policies must consider social impacts and how society can contribute to national security through the use of digital technology.

This network visualization also reveals the importance of international collaboration in managing digital transformation and national security. The relationships between countries such as the United States, China, and Russia show that these issues are not confined to a single country but require a global approach. These countries have different policies and strategies, but the challenges faced in the digital era are universal and require international cooperation to address threats and leverage opportunities. This network visualization provides a comprehensive overview of how various topics and concepts in the literature on digital transformation and national security are interrelated. It shows that research in this field is highly multidisciplinary, encompassing social, technical, strategic, and administrative aspects. By understanding these relationships, researchers and policymakers can develop more holistic and effective approaches to managing digital transformation and ensuring national security in the continually evolving digital era.

4.2.2. Co-authorship Analysis Visualization

Figure 6 presents a co-authorship analysis generated using VOSviewer software, illustrating collaborative relationships among various authors in the context of research on digital transformation and national security issues. Each node in the visualization represents an author, while the lines connecting the nodes indicate publication collaborations. This visualization reveals clusters of authors who frequently collaborate on this topic. Different colors in each cluster denote groups of authors who are closely connected, reflecting the collaborative networks within this academic community. The size of each author's circle also signifies the number of publications or contributions they have made in this field, with larger circles indicating more significant contributions.

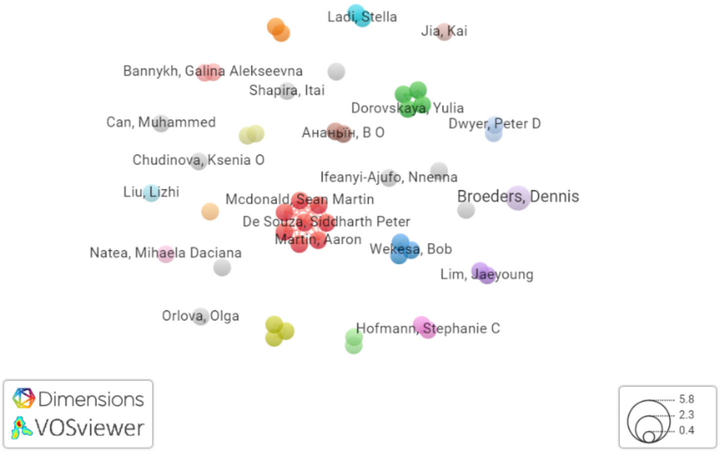


Figure 6. Network co-authorship analysis – Vosviewer.

One prominent author in this visualization is Dennis Broeders, who has a notably large circle, indicating his status as a major contributor to digital transformation and national security research. Broeders' connections with other authors in this visualization suggest that he has an extensive collaborative network, working with various researchers to advance studies in this field. Other authors who also appear to have significant contributions include Sean Martin, Ifeanyi-Ajufor Nnenna, and De Souza Siddharth Peter. These authors are part of the same cluster, demonstrating their frequent collaboration in related research. The collaboration among these authors indicates that research on digital transformation and national security involves diverse perspectives and expertise, enabling a richer exchange of ideas and innovations. Additionally, some authors appear to work in smaller groups or even independently, such as Ladi Stella and Jia Kai. This indicates various approaches to research on this topic, where some authors might focus more on independent research or collaboration within limited groups. This diversity in research approaches highlights the multifaceted nature of digital transformation and national security studies.

The visualization also illustrates international connections in research on digital transformation and national security. The names of authors from various backgrounds and countries reflect that this issue is of global concern, requiring cross-national and cross-cultural collaboration. For instance, authors like Bannykh Galina Alekseevna and Chudinova Ksenia O indicate participation from Russian researchers, while Can Muhammed's background suggests contributions from the Middle East or Asia. The geographical and institutional diversity among the authors is noteworthy. The names of authors from different backgrounds and countries indicate that research on digital transformation and national security is a global issue necessitating international cooperation. This is crucial for understanding that security issues in the digital age are not confined to one country or region but require global collaboration to find effective solutions.

Understanding co-authorship analysis is vital for comprehending how research in this field evolves and identifying key contributors. By recognizing these collaborative networks, we can pinpoint leading research centers and understand the relationships between various researchers and institutions that contribute to the knowledge of digital transformation and national security. This visualization clearly depicts the collaborative networks in research on digital transformation and national security issues. It shows that research in this field is not conducted in isolation but through intensive collaboration among authors from diverse backgrounds and countries. These collaborative networks facilitate a more effective exchange of knowledge and ideas, ultimately accelerating research progress and solutions to the challenges of digital transformation and national security. Analyzing co-authorship is crucial for understanding the dynamics within the academic community and identifying key research centers and contributors to developing knowledge on digital transformation and national security.

4.3. Future Direction and Implication

The discussion on the future direction and implications in the context of the bibliometric analysis results on the theme of Digital Transformation on National Security Strategy reveals several critical areas that require further attention. The findings, which include research trends and network analysis results from VOSviewer, provide a comprehensive view of the evolution of relevant themes in this field and how they interrelate. These findings highlight various interconnected and evolving themes, indicating how this field will continue to develop and its implications for future policy and practice.

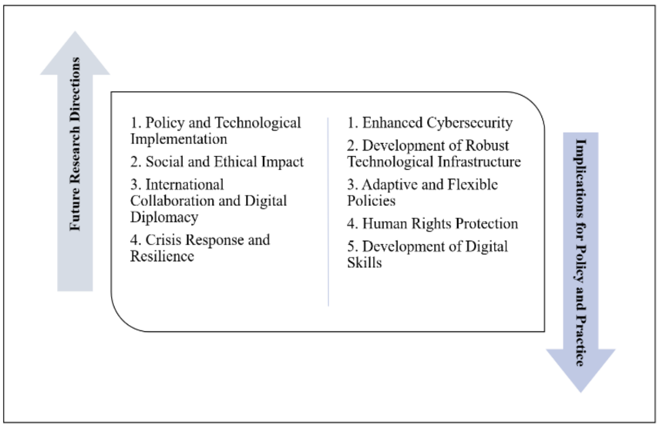

Future Research Directions
1. Policy and Technological Implementation
2. Social and Ethical Impact
3. International Collaboration and Digital Diplomacy
4. Crisis Response and Resilience
1. Enhanced Cybersecurity
2. Development of Robust Technological Infrastructure
3. Adaptive and Flexible Policies
4. Human Rights Protection
5. Development of Digital Skills
Implications for Policy and Practice

Figure 7. The schematic of future directions and implications – authors.

4.3.1. Future Research Directions

4.3.1.1. Policy and Technological Implementation

Future research should focus on how strategic policies can be integrated with the implementation of digital technologies to enhance national security. The visualization shows the importance of the relationship between policy, strategy, and implemented systems. Research should investigate how policies can support the development of technologies such as artificial intelligence (AI) and how these technologies can be implemented securely and effectively within the national security context.

4.3.1.2. Social and Ethical Impact

Digital transformation impacts not only technology but also social structures and ethics. The connection between “society” and “national security” indicates the need for further research on the social impact of digital technology adoption. This research should include analyses of how digital technologies can be implemented fairly and ethically, ensuring that this transformation benefits all societal layers equitably and does not exacerbate social inequalities.

4.3.1.3. International Collaboration and Digital Diplomacy

The inter-country relationships in the visualization indicate that international collaboration is crucial in addressing increasingly complex national security challenges. Future research should explore ways to enhance international cooperation in cybersecurity, including information sharing, developing global standards, and conducting joint training. Digital diplomacy is also an important area where countries can collaborate to build a stronger global framework for digital security.

4.3.1.4. Crisis Response and Resilience

The emergence of the “crisis” theme suggests that responding to emergencies is becoming increasingly important in the digital age. Future research needs to focus on how digital technologies can be used to respond to crises more efficiently, whether they are health crises, natural disasters, or security threats. Developing rapid response systems using advanced technologies such as AI and data analytics will be crucial to ensuring national resilience and sustainability.

4.3.2. Implications for Policy and Practice

4.3.2.1. Enhanced Cybersecurity

With increasing reliance on digital technologies, cybersecurity must be a top priority in national security strategies. Policymakers need to develop regulations and policies that support robust cybersecurity measures, including data protection and privacy, and enhance the capacity to detect and respond to cyber threats. This also includes investing in education and training to equip the workforce with the necessary skills to handle cybersecurity threats.

4.3.2.2. Development of Robust Technological Infrastructure

The implementation of digital technologies in the public sector and administration requires resilient technological infrastructure. Policies should focus on developing and maintaining technological infrastructure that can support widespread digital technology adoption. This includes reliable internet networks, secure cloud systems, and accessible digital platforms for all societal layers.

4.3.2.3. Adaptive and Flexible Policies

Digital transformation moves quickly, and rigid policies may not keep up with the pace of technological change. Policymakers should develop frameworks that are adaptive and flexible, capable of quickly adjusting to new developments in digital technology. This includes a principle- and outcome-based regulatory approach rather than strict rules.

4.3.2.4. Human Rights Protection

The implementation of digital technologies must consider human rights protection, including privacy, freedom of expression, and access to information. Policies should ensure that digital technologies are used ethically and responsibly and that mechanisms are in place to address human rights violations that may arise from using these technologies.

4.3.2.5. Development of Digital Skills

Digital transformation requires a workforce skilled in digital technologies. Educational and training programs should be tailored to ensure that individuals have the skills to participate in the digital economy. This includes data analytics, software development, cybersecurity, and technology management training.

Theoretically, this research makes a significant contribution to the literature on digital transformation and national security strategy by identifying key trends, thematic developments, and new research areas. The use of bibliometric analysis in this research expands understanding of how digital technologies, such as artificial intelligence, blockchain, and cybersecurity measures, influence national defence strategies. Through this study, a new theoretical framework was developed that integrates digital technologies in national security strategy. This framework includes a multidimensional approach to national security that involves advanced technologies to enhance capabilities, decision-making, and response to new threats. From a practical perspective, this research also offers strategic recommendations for policymakers in managing the complexity of the digital landscape while effectively strengthening national security. This includes the importance of adaptive policies that encourage innovation while ensuring resilience to evolving threats. Thus, this research not only contributes to the growing literature on digital transformation but also provides practical insights that can assist policymakers in devising more effective and adaptive national security strategies in this digital era. However, methodologically this research has limitations. Bibliometric methods tend to provide a general overview of literature trends and patterns. This method does not analyze the content or research results in depth, so it can ignore the specific context or substance in the studies or articles being analyzed. Furthermore, there are also limitations in predictions or projections. This research is not fully able to predict or project future trends regarding the relationship between digital transformation and national security strategy. This is due to the rapid evolution of technology and national security threats that continue to grow. Even though this research has several limitations, this research can become a catalyst for studies regarding digital transformation and national security. This research is quite capable of bridging national security issues in an era of massive adaptation to digital technology.

5. Conclusion

The bibliometric analysis provides deep insights into the evolution of themes related to digital transformation and national security strategy and how research in this field is distributed across various disciplines and countries. The study identifies the dominance of certain themes such as national security, digital transformation, strategy, and public policy implementation, all of which strongly focus on how digitalization impacts critical aspects of national security. The prominence of these themes reflects the academic community's significant attention to the complexity and importance of this topic in an increasingly digitally connected global context. Furthermore, the analysis reveals that social sciences and computer science fields play major roles in this research, indicating the multidisciplinary approach required to understand and address the challenges faced. Social sciences contribute to understanding digital transformation's social and policy impacts, while computer science focuses on the technical aspects and innovative solutions to enhance national security. The study also finds that countries such as China and the United Kingdom are major contributors to research in this area, highlighting the important role these countries play in developing and implementing digital-based national security strategies. The conclusion of this analysis emphasizes that digital transformation has broad and complex implications for national security strategy. It requires interdisciplinary and international collaboration to develop a comprehensive understanding and effective solutions. Future research must continue to explore the interaction between digital technologies and security policies and their impact on global stability and security. To address the challenges and leverage the opportunities presented by the digital era, researchers, policymakers, and practitioners need to work together to develop adaptive and innovative strategies. We can ensure that digital transformation brings maximal benefits to national security and global stability through a holistic and coordinated approach. The research has limitations, as bibliometric methods offer a general overview of literature trends but do not deeply analyze content. Predicting future trends on digital transformation and national security strategy is challenging due to rapid technological evolution and growing security threats. Despite these limitations, the research can inspire further studies on digital transformation and national security, bridging the gap in an era of extensive digital technology adaptation.

References

Abbu, H., Mugge, P., & Gudergan, G. (2024). *Ethical considerations of artificial intelligence: ensuring fairness, transparency, and explainability*. 1–7. https://doi.org/10.1109/ice/itmc-iamot55089.2022.10033140

Abd Al Ghaffar, H. t. A. N. (2024). Government cloud computing and national security. *Review of Economics and Political Science*, *9*(2), 116–133. https://doi.org/10.1108/REPS-09-2019-0125

Acemoglu, D., & Restrepo, P. (2019). Automation and new tasks: How technology displaces and reinstates labor. *Journal of Economic Perspectives*, *33*(2), 3–30. https://doi.org/10.1257/jep.33.2.3

Adigwe, C. S., Mayeke, N. R., Olabanji, S. O., Okunleye, O. J., Joeaneke, P. C., & Olaniyi, O. O. (2024). The evolution of terrorism in the digital age: Investigating the adaptation of terrorist groups to cyber technologies for recruitment, propaganda, and cyberattacks. *Asian Journal of Economics, Business and Accounting*, *24*(3), 289–306. https://doi.org/10.9734/ajeba/2024/v24i31287

Adisa, T. A., & Mordi, C. (2022). HRM in the global south: A critical perspective. In *HRM in the Global South: A Critical Perspective*. https://doi.org/10.1007/978-3-030-98309-3

Agarwala, N., & Chaudhary, R. D. (2021a). Artificial Intelligence and International Security. In *International Political Economy Series*. Center for a New American Security. https://doi.org/10.1007/978-3-030-74420-5_11

Agarwala, N., & Chaudhary, R. D. (2021b). 'Made in China 2025': Poised for success? *India Quarterly*, *77*(3), 424–461.

Ahad, M. A., Casalino, G., & Bhushan, B. (2023). Enabling Technologies for effective planning and management in sustainable smart cities. In *Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities*. https://doi.org/10.1007/978-3-031-22922-0

Aisenberg, M. A. (2018). State and local ICT policy: A framework for cybersecurity. *Scitech Lawyer*, *14*(3), 14–19. https://go.openathens.net/redirector/gatech.edu?url=https://search proquest.com/ docview/2088918742?accountid=11107

Akande, A. (2023). Globalization, human rights and populism: reimagining people, power and places. In *Globalization, Human Rights and Populism: Reimagining People, Power and Places*. https://doi.org/10.1007/978-3-031-17203-8

Akberdina, V., & Osmonova, A. (2021). Digital transformation of energy sector companies. *E3S Web of Conferences*, *250*, 6001.

Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, P. S. (2015). Application of big data for national security: A practitioner's guide to emerging technologies. In *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*. Butterworth-Heinemann. https://doi.org/10.1016/C2014-0-01051-9

Al-Suqri, M. N., & Gillani, M. (2022). A comparative analysis of information and artificial intelligence toward national security. *IEEE Access*, *10*, 64420–64434. https://doi.org/10.1109/ACCESS.2022.3183642

Alareeni, B. A. M., & Elgedawy, I. (2023). *Artificial Intelligence (AI) and finance*. https://doi.org/10.1007/978-3-031-39158-3

Alguliyev, R. M., Imamverdiyev, Y. N., Mahmudov, R. S., & Aliguliyev, R. M. (2020). Information security as a national security component. *Information Security Journal*, *30*(1), 1–18. https://doi.org/10.1080/19393555.2020.1795323

Allen, G. C. (2019). *Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security*.

Alqadhi, B., Hamdan, A., & Nasseif, H. (2023). Artificial Intelligence for decision making in the era of big data. *Lecture Notes in Networks and Systems*, *620 LNNS*, 604–612. https://doi.org/10.1007/978-3-031-26953-0_55

An, P. A. (2022). The evolution of cyber security threats in the digital age. *International Journal of Business Management and Visuals*, *5*(2), 22–29. https://ijbmv.com/index.php/home/article/view/20

Anunciação, Pessoa, & Jamil. (2021). Digital transformation and challenges to data security and privacy. In *Turpin Distribution*. IGI Global.

Argyroudis, S. A., Mitoulis, S. A., Chatzi, E., Baker, J. W., Brilakis, I., Gkoumas, K., Vousdoukas, M., Hynes, W., Carluccio, S., Keou, O., Frangopol, D. M., & Linkov, I. (2022). Digital technologies can enhance climate resilience of critical infrastructure. *Climate Risk Management*, *35*, 100387. https://doi.org/10.1016/j.crm.2021.100387

Asmorowati, S., Setijaningrum, E., Suaedi, F., & Fatmawati Dewi, Y. (2019). Smart governance in public financial management: A study of Government Resources Management System (GRMS) in the City of Surabaya. *Iapa Proceedings Conference*, 481. https://doi.org/10.30589/proceedings.2019.249

Banafa, A. (2020). Blockchain technology and applications. In *Blockchain Technology and Applications*. https://doi.org/10.1201/9781003337393

Bannykh, G., & Kostina, S. (2021). Formation of digital competence of state servants in the conditions of government digitalisation: The problem statement. *KnE Social Sciences*, 236–245–236–245. https://doi.org/10.18502/kss.v5i2.8357

Bareis, J., & Katzenbach, C. (2022). Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science Technology and Human Values*, *47*(5), 855–881. https://doi.org/10.1177/01622439211030007

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *International Affairs*, *96*(3), 749–766. https://doi.org/10.1093/ia/iiz274

Baylis, J., & Wirtz, J. J. (2015). Introduction: Strategy in the contemporary world: In *Strategy in the Contemporary World*. Oxford University Press. https://doi.org/10.1093/hepl/9780198708919.003.0001

Bertola, P., & Teunissen, J. (2018). Fashion 4.0. Innovating fashion industry through digital transformation. *Research Journal of Textile and Apparel*, *22*(4), 352–369. https://doi.org/10.1108/RJTA-03-2018-0023

Bharat Vagadia. (2017). Digital disruption. for Economies, society, policy makers implications and opportunities and business leaders. In *Future of Business and Finance*. https://doi.org/10.1007/978-3-030-54494-2

Bilozubenko, V., Yatchuk, O., Wolanin, E., Serediuk, T., & Korneyev, M. (2022). *Comparison of the digital economy development parameters in the EU countries in the context of bridging the digital divide*.

Bogoyavlenska, Y., University, Z. P. S., & Prus, V. (2023). Digital transformation of business: Approaches to evaluation of performance, potential, management. *Black Sea Economic Studies*, *84*. https://doi.org/10.32782/bses.84-25

Bondarchuk P. (2021). Political sciences digitalization in the values system of public administration: National security aspect. *Sciences of Europe #*, *66*(66–3), 69–71. http://visnik.knteu.kiev.ua/index.php?op-

Bounfour, A. (2016). Digital futures, digital transformation. *Progress in IS. Cham. Springer International Publishing, Doi*, *10*, 973–978.

Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation and Governance*, *15*(4), 1092–1110. https://doi.org/10.1111/rego.12343

Brooks, S. G., & Wohlforth, W. C. (2015). The rise and fall of the great powers in the twenty-first century: China's rise and the fate of America's global position. *International Security*, *40*(3), 7–53.

Brown, I., & Marsden, C. T. (2023). *Regulating code: Good governance and better regulation in the information age*. MIT Press.

Brown, J. (2018). An alternative war: The development, impact, and legality of hybrid warfare conducted by the nation state. *Journal of Global Faultlines*, *5*(1–2), 58–82. https://doi.org/10.13169/jglobfaul.5.1-2.0058

Brummer, M., & Ueno, H. (2024). Crisis and choice in digital transformation: COVID-19 and the punctuated politics of government DX in Japan. *Asia Pacific Journal of Public Administration*, *ahead-of-p*(ahead-of-print), 1–32. https://doi.org/10.1080/23276665.2023.2282472

Brunetti, F., Matt, D. T., Bonfanti, A., De Longhi, A., Pedrini, G., & Orzes, G. (2020). Digital transformation challenges: strategies emerging from a multi-stakeholder approach. *TQM Journal*, *32*(4), 697–724. https://doi.org/10.1108/TQM-12-2019-0309

Bryson, J., & George, B. (2020). Strategic management in public administration. In *Oxford research encyclopedia: politics* (pp. 1–26). Oxford University Press.

Caplan, N. (2013). Cyber war: the challenge to national security. *Global Security Studies*, *4*(1).

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, *8*(1). https://doi.org/10.1093/cybsec/tyac014

Chawla, R. N., & Goyal, P. (2022). Emerging trends in digital transformation: a bibliometric analysis. *Benchmarking*, *29*(4), 1069–1112. https://doi.org/10.1108/BIJ-01-2021-0009

Chehabeddine, M., & Tvaronavičienė, M. (2020). Securing regional development. *Insights into Regional Development*, *2*(1), 430–442. https://doi.org/10.9770/ird.2020.2.1(3)

Chwiłkowska-Kubala, A., Cyfert, S., Malewska, K., Mierzejewska, K., & Szumowski, W. (2023). The impact of resources on digital transformation in energy sector companies. The role of readiness for digital transformation. *Technology in Society*, *74*, 102315.

Chygryn, O., Kolosok, S., & Hordiienko, V. (2022). Digital eco-energy: Patterns of achieving economic leadership, national security, and sustainability. *PRIZK International Conference-Novel Insights in the Leadership in Business and Economics After the COVID-19 Pandemic*, 329–341.

Cooper, R. N. (2019). Digital transformation: Survive and thrive in an era of mass extinction by Thomas M. Siebel. In *Foreign Affairs* (Vol. 98, Issue 6). RosettaBooks.

Cunliffe, K. (2016). The new era in us national security: An introduction to emerging threats and challenges . In *Intelligence and National Security* (Vol. 31, Issue 2). Rowman & Littlefield. https://doi.org/10.1080/02684527.2015.1008208

Dąbrowska, J., Almpanopoulou, A., Brem, A., Chesbrough, H., Cucino, V., Di Minin, A., Giones, F., Hakala, H., Marullo, C., Mention, A. L., Mortara, L., Nørskov, S., Nylund, P. A., Oddo, C. M., Radziwon, A., & Ritala, P. (2022). Digital transformation, for better or worse: a critical multi-level research agenda. *R and D Management*, *52*(5), 930–954. https://doi.org/10.1111/radm.12531

Darıcılı, A. B., & Çelik, S. (2021). National Security 2.0: The Cyber Security of Critical Infrastructure. *PERCEPTIONS: Journal of International Affairs*, *XXVI*(2), 259–276. https://dergipark.org.tr/en/pub/perception/issue/68005/1055264%0Ahttps://dergipark.org.tr/en/download/article-file/2181981

Dear, K. (2022). Beyond the 'Geo' in Geopolitics: The Digital Transformation of Power. *RUSI Journal*, *166*(6–7), 20–31. https://doi.org/10.1080/03071847.2022.2049167

Demchak, C. C., & Dombrowski, P. J. (2014). Rise of a Cybered Westphalian Age: The Coming Decades. *Global Power Shift*, 91–113. https://doi.org/10.1007/978-3-642-55007-2_5

DeNardis, L. (2014). The global war for internet governance. In *The Global War for Internet Governance*. books.google.com. https://doi.org/10.2307/j.ctt5vkz4n

Denning, D. E. (2014). Framework and principles for active cyber defense. *Computers and Security*, *40*, 108–113. https://doi.org/10.1016/j.cose.2013.11.004

Dimitrov, W. (2020). Analysis of the Need for Cyber Security Components in the Study of Advanced Technologies. *INTED2020 Proceedings*, *1*, 5259–5268. https://doi.org/10.21125/inted.2020.1423

Dommett, K. (2020). Roadblocks to interactive digital adoption? Elite perspectives of party practices in the United Kingdom. *Party Politics*, *26*(2), 165–175.

Doukidis, G., Spinellis, D., & Ebert, C. (2020). Digital Transformation?A Primer for Practitioners. *IEEE Software*, *37*(5), 13–21. https://doi.org/10.1109/MS.2020.2999969

Douzet, F., & Gery, A. (2021). Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace. *Journal of Cyber Policy*, *6*(1), 96–113. https://doi.org/10.1080/23738871.2021.1937253

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., … Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *57*. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

El-Kalash, K. I., Mohammed, S. B., & Ulu, D. (2018). *Harnessing ICT for national security and sustainable development in Nigeria*.

El Kadiri, S., Grabot, B., Thoben, K. D., Hribernik, K., Emmanouilidis, C., Von Cieminski, G., & Kiritsis, D. (2016). Current trends on ICT technologies for enterprise information systems. *Computers in Industry*, *79*, 14–33. https://doi.org/10.1016/j.compind.2015.06.008

ElMassah, S., & Mohieldin, M. (2020). Digital transformation and localizing the Sustainable Development Goals (SDGs). *Ecological Economics*, *169*, 106490. https://doi.org/10.1016/j.ecolecon.2019.106490

Enggarratri, I. D. (2021). Gender Relations, Globalization and Gender Empowerment: The Implementation of Indonesia Digital Energy of Asia. *Kafaah: Journal of Gender Studies*, *11*(1), 1–14.

Fatimah, Y. A., Govindan, K., Murniningsih, R., & Setiawan, A. (2020). Industry 4.0 based sustainable circular economy approach for smart waste management system to achieve sustainable development goals: A case study of Indonesia. *Journal of Cleaner Production*, *269*, 122263.

Favoretto, C., Mendes, G. H. de S., Filho, M. G., Gouvea de Oliveira, M., & Ganga, G. M. D. (2022). Digital transformation of business model in manufacturing companies: challenges and research agenda. *Journal of Business and Industrial Marketing*, *37*(4), 748–767. https://doi.org/10.1108/JBIM-10-2020-0477

Fedotova, G. V., Kovalenko, O. A., Malyutina, T. D., Glushchenko, A. V., & Sukhinin, A. V. (2019). Transformation of information security systems of enterprises in the context of digitization of the national economy. *Studies in Computational Intelligence*, *826*, 811–822. https://doi.org/10.1007/978-3-030-13397-9_84

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2013). Embracing Digital Technology: A New Strategic Imperative. *MIT Sloan Management Review*, *55*(2), 1–12.

Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalisation. *Resilience*, *2*(2), 114–129. https://doi.org/10.1080/21693293.2014.914771

Galinec, D., Moznik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika*, *58*(3), 273–286. https://doi.org/10.1080/00051144.2017.1407022

Geels, F. W. (2013). The impact of the financial–economic crisis on sustainability transitions: Financial investment, governance and public discourse. *Environmental Innovation and Societal Transitions*, *6*, 67–95.

Gilli, A., & Gilli, M. (2018). Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. *International Security*, *43*(3), 141–189.

Gray, J. E. (2021). The geopolitics of 'platforms': The tiktok challenge. *Internet Policy Review*, *10*(2), 1–26. https://doi.org/10.14763/2021.2.1557

Grisales Rendón, L. (2022). Latin American eGovernance and data protection: the EU model. *ACM International Conference Proceeding Series*, 100–105. https://doi.org/10.1145/3551504.3551558

Guitton, C. (2013). Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *European Security*, *22*(1), 21–35.

Gulley, A. L., Nassar, N. T., & Xun, S. (2018). China, the United States, and competition for resources that enable emerging technologies. *Proceedings of the National Academy of Sciences*, *115*(16), 4111–4115.

Gupta, I., & Pathak, P. (2022). Cybersecurity in digital epoch: Emerging threats and modern defense techniques. *AIP Conference Proceedings*, *2519*(1). https://doi.org/10.1063/5.0109715

Hai, T. N., Van, Q. N., & Tuyet, M. N. T. (2021). Digital Transformation: Opportunities and Challenges for Leaders in the Emerging Countries in Response to Covid-19 Pandemic. *Emerging Science Journal*, *5*(0), 21–36. https://doi.org/10.28991/esj-2021-sper-03

Hajishirzi, R., Costa, C. J., Aparicio, M., & Romão, M. (2022). Digital Transformation Framework: A Bibliometric Approach. In *Lecture Notes in Networks and Systems: Vol. 470 LNNS* (pp. 427–437). https://doi.org/10.1007/978-3-031-04829-6_38

Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change. *Journal of Management Studies*, *58*(5), 1159–1197. https://doi.org/10.1111/joms.12639

Hanna, N. (2018). A role for the state in the digital age. In *Journal of Innovation and Entrepreneurship* (Vol. 7, Issue 1). innovation-entrepreneurship …. https://doi.org/10.1186/s13731-018-0086-3

Harris, S. (2014). *@ War: the rise of the military-internet complex*. Houghton Mifflin Harcourt.

Hartanto, D., Agussani, A., & Dalle, J. (2021). Antecedents of public trust in government during the COVID-19 pandemic in Indonesia: Mediation of perceived religious values. *Journal of Ethnic and Cultural Studies*, *8*(4), 321–341. https://doi.org/10.29333/EJECS/975

He, A. J., Shi, Y., & Liu, H. (2020). Crisis governance, Chinese style: distinctive features of China's response to the Covid-19 pandemic. *Policy Design and Practice*, *3*(3), 242–258.

Heath, T., Gunness, K., & Cooper, C. (2017). The PLA and China's Rejuvenation: National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities. In *The PLA and China's Rejuvenation: National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities*. RAND Corporation Santa Monica, CA. https://doi.org/10.7249/rr1402

Hermeto, J. R. (2021). Towards Social Change: Social Transformation in a Time of Social Disruption. *Dilemas*, *14*(1), 219–242. https://doi.org/10.17648/DILEMAS.V14N1.30572

Hidayatno, A., Destyanto, A. R., & Hulu, C. A. (2019). Industry 4.0 technology implementation impact to industrial sustainable energy in Indonesia: A model conceptualization. *Energy Procedia*, *156*, 227–233.

Humm, G., Harries, R. L., Stoyanov, D., & Lovat, L. B. (2021). Supporting laparoscopic general surgery training with digital technology: the United Kingdom and Ireland paradigm. *BMC Surgery*, *21*(1), 123.

Hurel, L. M. (2022). Interrogating the Cybersecurity Development Agenda: A Critical Reflection. *The International Spectator*, *57*(3), 66–84. https://doi.org/10.1080/03932729.2022.2095824

Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation. *Policy Design and Practice*, *6*(2), 146–159. https://doi.org/10.1080/25741292.2023.2199960

Ilyina, E. M. (2022). Politics and Administration under Conditions of Digital Transformation: a Political Science Perspective of Artificial Intelligence. *Ars Administrandi (Искусство Управления)*, *14*(3), 403–421. https://doi.org/10.17072/2218-9173-2022-3-403-421

Ismail, Fathonih, A., Prabowo, H., Hartati, S., & Redjeki, F. (2020). Transparency and corruption: Does E-government effective to combat corruption? *International Journal of Psychosocial Rehabilitation*, *24*(4), 5396–5404. https://doi.org/10.37200/IJPR/V24I4/PR201636

Jagatheesaperumal, S. K., Rahouti, M., Ahmad, K., Al-Fuqaha, A., & Guizani, M. (2022). The Duo of Artificial Intelligence and Big Data for Industry 4.0: Applications, Techniques, Challenges, and Future Research Directions. *IEEE Internet of Things Journal*, *9*(15), 12861–12885. https://doi.org/10.1109/JIOT.2021.3139827

Jansen, B., Kadenko, N., Broeders, D., van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, *40*(4), 101862. https://doi.org/10.1016/j.giq.2023.101862

Jenkins, B. M., Liepman, A., & Willis, H. H. (2014). *Identifying Enemies Among Us: Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing*. RAND corporation.

Johnson, M. (2020). ICT and Cyber Security Risks in Telecoms. In *Demystifying Communications Risk* (pp. 187–208). Routledge. https://doi.org/10.4324/9781315576497-13

Judijanto, L., & Solapari, N. (2024). A Bibliometric Analysis of Legal Approaches to Personal Data Protection. *The Easta Journal Law and Human Rights*, *2*(03), 165–175.

Kache, F., & Seuring, S. (2017). Challenges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management. *International Journal of Operations and Production Management*, *37*(1), 10–36. https://doi.org/10.1108/IJOPM-02-2015-0078

Kadtke, J. B., & Wells, L. (2014). *Policy challenges of accelerating technological change: Security policy and strategy implications of parallel scientific revolutions*. Center for Technology and National Security Policy, National Defense University.

Kahler, M. (2013). Rising powers and global governance: Negotiating change in a resilient status quo. *International Affairs*, *89*(3), 711–729. https://doi.org/10.1111/1468-2346.12041

Kapitonov, I. A., Voloshin, V. I., Filosofova, T. G., & Syrtsov, D. N. (2020). Digitalization of the energy industry as a direction for ensuring the growth of energy efficiency and the energy security of the state. *Public Policy and Administration*, *19*(2), 191–204.

Karmous-Edwards, G., Tomic, S., & Cooper, J. P. (2022). Developing a Unified Definition of Digital Twins. *Journal - American Water Works Association*, *114*(6), 76–78. https://doi.org/10.1002/awwa.1946

Kello, L. (2023). The State in the Digital Era. *Digital International Relations*, 51–72. https://doi.org/10.4324/9781003437963-4

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3), 293–312.

Keping, Y. (2018). Governance and Good Governance: A New Framework for Political Analysis. *Fudan Journal of the Humanities and Social Sciences*, *11*(1), 1–8. https://doi.org/10.1007/s40647-017-0197-4

Kettl, D. F. (2015). The transformation of governance: public administration for the twenty-first century. In *Choice Reviews Online* (Vol. 53, Issue 01). books.google.com. https://doi.org/10.5860/choice.192390

Khan, N., Lee, D., Alia, A. K., & Park, C. (2020). Artificial intelligence and blockchain-based inspection data recording system for portable firefighting equipment. *Proceedings of the 37th International Symposium on Automation and Robotics in Construction, ISARC 2020: From Demonstration to Practical Use - To New Stage of Construction Robot*, *November*, 941–947. https://doi.org/10.22260/isarc2020/0130

Kormych, L., Krasnopolska, T., & Zavhorodnia, Y. (2024). Digital Transformation and National Security Ensuring. *Evropsky Politicky a Pravni Diskurz*, *11*(1), 29–37. https://doi.org/10.46340/eppd.2024.11.1.4

Kouroubali, A., & Katehakis, D. G. (2019). The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. *Journal of Biomedical Informatics*, *94*, 103166. https://doi.org/10.1016/j.jbi.2019.103166

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital Transformation: An Overview of the Current State of the Art of Research. *SAGE Open*, *11*(3). https://doi.org/10.1177/21582440211047576

Kravchenko, V. (2024). *An Assessment Threats to the Economic Security of a Region in the Digital Economy: A Case Study of Public Procurement in Russia* (pp. 3–12). https://doi.org/10.1007/978-3-031-32719-3_1

Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy*, *44*(6), 101976.

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022). Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(4), 195. https://doi.org/10.3390/joitmc8040195

Lee-Geiller, S., & Lee, T. (David). (2019). Using government websites to enhance democratic E-governance: A conceptual model for evaluation. *Government Information Quarterly*, *36*(2), 208–225. https://doi.org/10.1016/j.giq.2019.01.003

Lee, J. W. (2020). Big data strategies for government, society and policy-making. *Journal of Asian Finance, Economics and Business*, *7*(7), 475–487. https://doi.org/10.13106/jafeb.2020.vol7.no7.475

Legrand, T., & Leuprecht, C. (2021). Securing cross-border collaboration: transgovernmental enforcement networks, organized crime and illicit international political economy. *Policy and Society*, *40*(4), 565–586. https://doi.org/10.1080/14494035.2021.1975216

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. In *Computational Methods in Applied Sciences* (Vol. 56, pp. 3–42). Springer. https://doi.org/10.1007/978-3-030-91293-2_1

Lewis, T. G. (2019). *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.

Lindsay, J. R. (2014). The impact of China on cybersecurity: Fiction and friction. *International Security*, *39*(3), 7–47.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. Oxford University Press, USA.

Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2018). Governance strategies for a sustainable digital world. *Sustainability (Switzerland)*, *10*(2), 440. https://doi.org/10.3390/su10020440

Liu, S. M., & Yuan, Q. (2015). The Evolution of Information and Communication Technology in Public Administration. *Public Administration and Development*, *35*(2), 140–151. https://doi.org/10.1002/pad.1717

Liu, Y., Li, J., & Yang, Y. (2018). Strategic adjustment of land use policy under the economic transformation. *Land Use Policy*, *74*, 5–14.

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy*. CQ press.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6*, *9*(1–2), 3–31.

Mahor, V., Bijrothiya, S., Rawat, R., Kumar, A., Garg, B., & Pachlasiya, K. (2022). IoT and Artificial Intelligence Techniques for Public Safety and Security. In *Smart Urban Computing Applications* (pp. 111–126). River Publishers. https://doi.org/10.1201/9781003373247-5

Makarychev, A., & Wishnick, E. (2022). Anti-Pandemic Policies in Estonia and Taiwan: Digital Power, Sovereignty and Biopolitics. *Social Sciences*, *11*(3), 112. https://doi.org/10.3390/socsci11030112

Makhlooqa, A., & Mubarakb, M. Al. (2024). Artificial intelligence and marketing: Challenges and opportunities. In *Technological Innovations for Business, Education and Sustainability* (pp. 3–16). Qeios. https://doi.org/10.1108/978-1-83753-106-620241001

Makridakis, S. (2017). The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. *Futures*, *90*, 46–60.

Malikova, A. K., Dinorshoev, A. M., & Salokhidinova, S. M. (2022). Digital Transformation of Business Education. *Lecture Notes in Civil Engineering*, *210*(1), 461–467. https://doi.org/10.1007/978-3-030-90843-0_53

Mamediieva, G., & Moynihan, D. (2023). Digital resilience in wartime: The case of Ukraine. *Public Administration Review*, *83*(6), 1512–1516. https://doi.org/10.1111/puar.13742

Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale JL & Tech.*, *21*, 106.

Mao, Y., & Shi-Kupfer, K. (2021). Online public discourse on artificial intelligence and ethics in China: context, content, and implications. *AI & SOCIETY*, *38*(1), 373–389. https://doi.org/10.1007/s00146-021-01309-7

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: A quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *371*(1987). https://doi.org/10.1098/rsta.2012.0382

Maroufkhani, P., Desouza, K. C., Perrons, R. K., & Iranmanesh, M. (2022). Digital transformation in the resource and energy sectors: A systematic review. *Resources Policy*, *76*, 102622.

Maryanti, N., Rohana, R., & Kristiawan, M. (2020). The principal's strategy in preparing students ready to face the industrial revolution 4.0. *International Journal of Educational Review*, *2*(1), 54–69.

Masyhar, A., & Emovwodo, S. O. (2023). Techno-Prevention in Counterterrorism: Between Countering Crime and Human Rights Protection. *Journal of Human Rights, Culture and Legal System*, *3*(3), 625–655. https://doi.org/10.53955/jhcls.v3i3.176

Matos, F., Vairinhos, V., Salavisa Lança, I., Edvinsson, L., & Massaro, M. (2020). *Knowledge, People, and Digital Transformation Approaches for a Sustainable Future* . https://doi.org/10.1007/978-3-030-40390-4

Mayntz, R. (2017). From government to governance: Political steering in modern societies. In *Governance of integrated product policy* (pp. 18–25). Routledge.

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, *36*(4), 101385. https://doi.org/10.1016/j.giq.2019.06.002

Milakovich, M. E. (2021). *Digital governance: Applying advanced technologies to improve public service* (2nd ed.). Routledge. https://doi.org/10.4324/9781003215875

Mishra, S., & Gochhait, S. (2024). *Emerging Cybersecurity Attacks in the Era of Digital Transformation*. 1442–1447. https://doi.org/10.1109/iciccs56967.2023.10142357

Möller, D. P. F. (2023a). Cybersecurity in Digital Transformation. In *Advances in Information Security* (Vol. 103, pp. 1–70). https://doi.org/10.1007/978-3-031-26845-8_1

Möller, D. P. F. (2023b). Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices. In *Advances in information security*. https://doi.org/10.1007/978-3-031-26845-8

Mongeau, S., & Hajdasinski, A. (2021). *Cybersecurity Data Science, Best Practices in an Emerging Profession*. https://doi.org/10.1007/978-3-030-74896-8

Montasari, R. (2022). Artificial Intelligence and National Security. *Artificial Intelligence and National Security*, *45178*, 1–230. https://doi.org/10.1007/978-3-031-06709-9

Montasari, R. (2023). The Potential Impacts of the National Security Uses of Big Data Predictive Analytics on Human Rights. In *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity* (pp. 115–137). Springer.

Mori, S. (2019). US Technological Competition with China: The Military, Industrial and Digital Network Dimensions. *Asia-Pacific Review*, *26*(1), 77–120. https://doi.org/10.1080/13439006.2019.1622871

Mosco, V. (2017). *Becoming digital: Toward a post-internet society*. Emerald Publishing Limited.

Moussa, A., & Tarek, S. (2023). Digital Transformation and its Impact in Egypt: A Comprehensive Literature Review. *International Journal of Professional Business Review*, *8*(8), e02755–e02755. https://doi.org/10.26668/businessreview/2023.v8i8.2755

Mutanda, D. (2024). Social media and human development in Zimbabwe: opportunities and challenges. *Cogent Arts and Humanities*, *11*(1), 2313850. https://doi.org/10.1080/23311983.2024.2313850

Nalbantoğlu, C. (2022). EU - China relations and data governance policies: the role of civil societies in overcoming geopolitical challenges in cyberspace. *Cuadernos Europeos de Deusto*, *5*, 51–73. https://doi.org/10.18543/ced.2555

Nazari, Z., & Musilek, P. (2023). Impact of digital transformation on the energy sector: A review. *Algorithms*, *16*(4), 211.

Nguyen, D., Dekker, I., & Nguyen, S. (2020). Understanding media and society in the age of digitalisation. In *Understanding Media and Society in the Age of Digitalisation*. https://doi.org/10.1007/978-3-030-38577-4

Ohkubo, K. (2019). Cybersecurity Technologies Essential in the Digital Transformation Era. *International Journal of Informatics Society*, *11*(1), 13–21.

Oling, P., Rietjens, S., van Fenema, P., & Schakel, J. K. (2022). Towards a cultural perspective on the absorption of emerging technologies in military organizations. *Intelligence and National Security*, *37*(4), 482–497. https://doi.org/10.1080/02684527.2022.2065604

Omand, D. (2014). *Securing the state*. Oxford University Press.

Osei-Kojo, A. (2017). E-government and public service quality in Ghana. *Journal of Public Affairs*, *17*(3), e1620.

Owen, T. (2015). *Disruptive power: The crisis of the state in the digital age*. Oxford University Press, USA.

Parasol, M. (2018). The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams. *Computer Law & Security Review*, *34*(1), 67–98.

Paschal Uchenna, C. (2018). The Impact of ICT on National Security: A Case of Nigeria Security and Civil Defence Corps. *International and Public Affairs*, *2*(3), 48. https://doi.org/10.11648/j.ipa.20180203.11

Pătraşcu, P. (2021). Emerging Technologies and National Security: The Impact of IoT in Critical Infrastructures Protection and Defence Sector. *Land Forces Academy Review*, *26*(4), 423–429. https://doi.org/10.2478/raft-2021-0055

Paunov, C., & Guellec, D. (2024). *Artificial Intelligence: A Review of the Economic Context and Policy Agenda* (pp. 79–101). https://doi.org/10.1007/978-3-030-90192-9_4

Peng, B. (2022). Digital leadership: State governance in the era of digital technology. *Cultures of Science*, *5*(4), 210–225.

Pfeifer, J. W. (2012). Network Fusion: Information and Intelligence Sharing for a Networked World. *Homeland Security Affairs*, *8*(1).

Philip, L., Cottrill, C., Farrington, J., Williams, F., & Ashmore, F. (2017). The digital divide: Patterns, policy and scenarios for connecting the 'final few'in rural communities across Great Britain. *Journal of Rural Studies*, *54*, 386–398.

Poliakova, V. V, Sumbatyan, S. L., & Hakobyan, E. A. (2024). *Digital Platforms as a Business Engine in Smart Space* (pp. 587–594). https://doi.org/10.1007/978-3-030-56433-9_61

Popkova, E. G. (2022). *Correction to: Business 4.0 as a Subject of the Digital Economy*. https://doi.org/10.1007/978-3-030-90324-4_203

Prabawa, W. G., Mutiarin, D., Purnomo, E. P., & Roengtam, S. (2024). Bibliometric Analysis in the Development of Public Sector Digitalization. *Journal of Governance and Public Policy*, *11*(2), 114–126.

Preuveneers, D., Joosen, W., Bernal Bernabe, J., & Skarmeta, A. (2020). Distributed Security Framework for Reliable Threat Intelligence Sharing. *Security and Communication Networks*, *2020*(1), 8833765. https://doi.org/10.1155/2020/8833765

Pylypenko, V., Bondarenko, S., Kolisnichenko, R., Runcheva, N., Gorniak, K., & Drobotov, S. (2022). Information and Analytical Support Threat Monitoring and Means of Overcoming Challenges To National Security: International Legal Aspect. *Trames*, *26*(4), 373–395. https://doi.org/10.3176/tr.2022.4.02

Qiang, X. (2019). The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy*, *30*(1), 53–67.

Rackwitz, M., Hustedt, T., & Hammerschmid, G. (2021). Digital transformation: From hierarchy to network-based collaboration? The case of the German "Online Access Act." *Der Moderne Staat – Zeitschrift Für Public Policy, Recht Und Management*, *14*(1–2021), 101–120. https://doi.org/10.3224/dms.v14i1.05

Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, 1–51. https://doi.org/10.1080/23742917.2024.2312671

Rajavuori, M., & Huhta, K. (2020). Digitalization of security in the energy sector: evolution of EU law and policy. *The Journal of World Energy Law & Business*, *13*(4), 353–367.

Ren, Y., Li, B., & Liang, D. (2023). Impact of digital transformation on renewable energy companies' performance: Evidence from China. *Frontiers in Environmental Science*, *10*, 1105686. https://doi.org/10.3389/fenvs.2022.1105686

Retnandari, N. D. (2022). Implementation of strategic planning in regional/municipal governments, obstacles and challenges. *Policy & Governance Review*, *6*(2), 155–175.

Riva Sanseverino, E., Riva Sanseverino, R., & Anello, E. (2018). A cross-reading approach to smart city: A european perspective of chinese smart cities. *Smart Cities*, *1*(1), 26–52.

Roberts, P. S., & Schmid, J. (2022). Government-led innovation acceleration: Case studies of US federal government innovation and technology acceleration organizations. *Review of Policy Research*, *39*(3), 353–378. https://doi.org/10.1111/ropr.12474

Roy, J. (2006). E-government in Canada: Transformation for the digital age. In *E-Government in Canada: Transformation for the Digital Age*. University of Ottawa Press. https://doi.org/10.1353/book4431

Rubin, D., Lynch, K., Escaravage, J., & Lerner, H. (2014). Harnessing Data for National Security. *SAIS Review of International Affairs*, *34*(1), 121–128. https://doi.org/10.1353/sais.2014.0008

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), 453–481. https://doi.org/10.1080/08850607.2013.780552

Rustiarini, N. W. (2019). The role of e-government in reducing corruption: A systematic review. *Jurnal Perspektif Pembiayaan Dan Pembangunan Daerah*, *7*(3), 269–286. https://doi.org/10.22437/ppd.v7i3.8311

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67.

Saner, R., Yiu, L., & Nguyen, M. (2020). Monitoring the SDGs: Digital and social technologies to ensure citizen participation, inclusiveness and transparency. *Development Policy Review*, *38*(4), 483–500. https://doi.org/10.1111/dpr.12433

Saranov, N. (2019). Cooperation Model for Establishing Secure Digital Transformation in Corporations: Overview of Regulatory Issues. *Information & Security: An International Journal*, *43*(1), 98–112. https://doi.org/10.11610/isij.4309

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, *39*(4), 101679.

Saxena, R., & Gayathri, E. (2021). Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. *Materials Today: Proceedings*, *51*, 682–689. https://doi.org/10.1016/j.matpr.2021.06.204

Sayler, K. M. (2020). Artificial intelligence and national security. *Congressional Research Service*, *45178*.

Senol, M., & Karacuha, E. (2020). Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering (United Kingdom)*, *2020*(1), 5267564. https://doi.org/10.1155/2020/5267564

Shackelford, S. J., & Craig, A. N. (2014). Beyond the new "digital divide": Analyzing the evolving role of national governments in Internet governance and enhancing cybersecurity. *Stanford Journal of International Law*, *50*(1), 119–184.

Shafqat, N., & Masood, A. (2016). Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security (IJSIS)*, *14*(1), 129–136.

Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. *Revista Espanola de Documentacion Cientifica*, *15*(4), 42–66. https://redc.revistas-csic.com/index.php/Jorunal/article/view/156

Shahzad Akram, M. (2023). Digital Shadows: The Menace of Cyber Espionage and Pakistan's National Security. *Journal of Development and Social Sciences*, *4*(III), 855–864. https://doi.org/10.47205/jdss.2023(4-iii)80

Shakarishvili, D., & Tbilisi, G. (2024). *Business Intelligence Management and its Impact on Economic Security*. 419–429. https://doi.org/10.18690/um.epf.5.2022.40

Shi, L., Mai, Y., & Wu, Y. J. (2022). Digital Transformation. *Journal of Organizational and End User Computing*, *34*(7), 1–20. https://doi.org/10.4018/JOEUC.302637

Singh, S., & Singh, R. (2022). Economic Imperatives of Evolving National Digital Policy: A Call for a Modern Industrial Policy Framework in India. *The International Trade Journal*, *36*(6), 572–593. https://doi.org/10.1080/08853908.2022.2041508

Smolarek, M., & Witkowski, M. (2015). Ict Security Of A State. *International Conference KNOWLEDGE-BASED ORGANIZATION*, *21*(3), 743–748. https://doi.org/10.1515/kbo-2015-0125

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics (Switzerland)*, *9*(11), 1–31. https://doi.org/10.3390/electronics9111864

Soesanto, S. (2023). Ukraine's IT Army. *Survival*, *65*(3), 93–106. https://doi.org/10.1080/00396338.2023.2218701

Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, *5*(3), 392–412.

Ştefan, M. (2022). Agile approaches to developing e-Business solutions in a secure cyber environment. *Proceedings of the International Conference on Business Excellence*, *16*(1), 239–250. https://doi.org/10.2478/picbe-2022-0023

Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs*, *92*(5), 1079–1105.

Strand, S. (2016). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. In *Internasjonal Politikk* (Vol. 74, Issue 4). Hachette UK. https://doi.org/10.17585/ip.v74.622

Su, C., & Flew, T. (2020). The rise of Baidu, Alibaba and Tencent (BAT) and their role in China's Belt and Road Initiative (BRI). *Global Media and Communication*, *17*(1), 67–86. https://doi.org/10.1177/1742766520982324

Sun, J. (2024). *Chapter 5 Urban risk prevention-and-control system and capacity building* (pp. 185–224). https://doi.org/10.1016/b978-0-443-18642-4.00006-3

Syed, F. Z., & Javed, S. (2017). Deterrence: A Security Strategy against Non Traditional Security Threats to Pakistan. *International Journal of Social Sciences and Management*, *4*(4), 267–274. https://doi.org/10.3126/ijssm.v4i4.18503

Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, *40*(2), 137–157.

Tatar, Ü., Çalik, O., Çelik, M., & Karabacak, B. (2014). A comparative analysis of the national cyber security strategies of leading nations. *International Conference on Cyber Warfare and Security*, 211.

Thanh, T. T., Ha, L. T., Dung, H. P., & Huong, T. T. L. (2023). Impacts of digitalization on energy security: evidence from European countries. *Environment, Development and Sustainability*, *25*(10), 11599–11644.

Tomczyk, Ł., Guillén-Gámez, F. D., Ruiz-Palmero, J., & Habibi, A. (2023). *From digital divide to digital inclusion: Challenges, perspectives and trends in the development of digital competences*. https://doi.org/10.1007/978-981-99-7645-4

Tran-Dang, H., & Kim, D. S. (2021). The Physical Internet in the Era of Digital Transformation: Perspectives and Open Issues. *IEEE Access*, *9*, 164613–164631. https://doi.org/10.1109/ACCESS.2021.3131562

Tropina, T., & Callanan, C. (2015). Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. In *SpringerBriefs in Cybersecurity*. Springer. http://link.springer.com/10.1007/978-3-319-16447-2

Tsaruk, O., & Korniiets, M. (2020). Hybrid nature of modern threats for cybersecurity and information security. *Smart Cities and Regional Development (SCRD) Journal*, *4*(1), 57–78. https://econpapers.repec.org/RePEc:pop:journl:v:4:y:2020:i:1:p:57-78

Tuskov, A. A., University of technologies and management, K. G. R. M. S., Spiridonova, A. A., & University, P. S. (2023). Digital economy formation and development at the regional level. *Izvestiya of Saratov University. Economics. Management. Law*, *23*(4), 420–427. https://doi.org/10.18500/1994-2540-2023-23-4-420-427

Upadhyay, P. (2023). Information Warfare and Digitalization of Politics in a Globalized World. *Journal of Political Science*, 1–30. https://doi.org/10.3126/jps.v23i1.52280

Valle-Cruz, D. (2019). Public value of e-government services through emerging technologies. *International Journal of Public Sector Management*, *32*(5), 473–488. https://doi.org/10.1108/IJPSM-03-2018-0072

Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, *52*(3), 326–349. https://doi.org/10.1016/j.lrp.2018.12.001

Weber-Lewerenz, B. C. (2022). *Accents of added value in construction 4.0, Ethical observations in dealing with digitization and AI*. https://doi.org/10.1007/978-3-658-39407-3

Wei, J., & Wang, C. (2021). Improving interaction mechanism of carbon reduction technology innovation between supply chain enterprises and government by means of differential game. *Journal of Cleaner Production*, *296*. https://doi.org/10.1016/j.jclepro.2021.126578

Weissmann, M., Nilsson, N., Palmertz, B., & Thunholm, P. (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. Bloomsbury Academic. https://doi.org/10.5040/9781788317795

Wiklund, J. (2022). Working in Bed—A Commentary on "Automation, Algorithms, and Beyond: Why Work Design Matters More than Ever in a Digital World" by Parker and Grote. *Applied Psychology*, *71*(4), 1210–1214. https://doi.org/10.1111/apps.12261

Wübbeke, J., Meissner, M., Zenglein, M. J., Ives, J., & Conrad, B. (2016). Made in china 2025. *Mercator Institute for China Studies. Papers on China*, *2*(74), 4.

Xin, L., Sun, H., & Xia, X. (2022). Renewable energy technology innovation and inclusive low-carbon development from the perspective of spatiotemporal consistency. *Environmental Science and Pollution Research*, *30*(8), 20490–20513. https://doi.org/10.1007/s11356-022-23556-x

Xu, Y., Ge, W., Liu, G., Su, X., Zhu, J., Yang, C., Yang, X., & Ran, Q. (2023). The impact of local government competition and green technology innovation on economic low-carbon transition: new insights from China. In *Environmental Science and Pollution Research* (Vol. 30, Issue 9, pp. 23714–23735). Springer. https://doi.org/10.1007/s11356-022-23857-1

Yang, J.-S., Lee, H.-J., Park, M.-W., & Eom, J. (2015). Security Threats on National Defense ICT based on IoT. *Advanced Science and Technology Letters*, *97*, 94–98. https://doi.org/10.14257/astl.2015.97.16

Yao, S., & Fu, Z. (2023). Can digital transformation promote the improvement of regional food security? Empirical findings from China. *Agribusiness*. https://doi.org/10.1002/agr.21881

Yeganegi, K., Arbabi, Z., & Hussein, A. I. (2020). The role of information technology in national security. *Journal of Physics: Conference Series*, *1530*(1), 6–14. https://doi.org/10.1088/1742-6596/1530/1/012112

Yeung, H. W. (2013). Regional development and the competitive dynamics of global production networks: an East Asian perspective. In *Globalizing Regional Development in East Asia* (pp. 5–31). Routledge.

Yu, F., Zhang, Q., & Jiang, D. (2023). The impact of regional environmental regulations on digital transformation of energy companies: The moderating role of the top management team. *Managerial and Decision Economics*, *44*(6), 3152–3165. https://doi.org/10.1002/mde.3868

Zaki, M. (2019). Digital transformation: harnessing digital technologies for the next generation of services. *Journal of Services Marketing*, *33*(4), 429–435. https://doi.org/10.1108/JSM-01-2019-0034

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, *8*, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

Zenglein, M. J., & Holzmann, A. (2019). Evolving made in China 2025. *MERICS Papers on China*, *8*, 78.

Zhang, F., Cui, Y., & Campbell-Verduyn, M. (2023). Digital RMB vs. Dollar Hegemony? Friendly Foes in China-US Currency Competition. *Journal of Chinese Political Science*, 1–26. https://doi.org/10.1007/s11366-023-09876-w

Zhao, M. (2019). Is a new Cold War inevitable? Chinese perspectives on US–China strategic competition. *The Chinese Journal of International Politics*, *12*(3), 371–394.

Zhong, M., Ali, M., Faqir, K., Begum, S., Haider, B., Shahzad, K., & Nosheen, N. (2022). China Pakistan Economic Corridor Digital Transformation. *Frontiers in Psychology*, *13*, 887848. https://doi.org/10.3389/fpsyg.2022.887848