Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 4 Issue 3 (2024)

Technological Innovations and Global Security: Risks and Opportunities

Ms. Priyanka Nehra[1]
Assistant Professor, Department of Commerce
Chandigarh Business School Administration, Cgc , Landran ,Mohali, Punjab, India - 140307
priyanka.5126@cgc.edu.in

Dr. J. Bamini[2]
Director, Department of Management Studies
SNS College of Technology, Coimbatore
baminikar@gmail.com

Neha Choudhary[3]
Assistant Professor, Amity School of Management and Commerce,
Amity University Jharkhand
nehacdbg@gmail.com

Dr R K Sant[4]
Professor
Maharaja Agrasen College, Delhi -110096
rksant@mac.du.ac.in

Swapna Datta Khan[5]
Associate Professor, NSHM Business School
NSHM Knowledge Campus, 60 BL Saha Road, Kolkata 700053
captsdk@gmail.com

Dr Neeti Mathur[6]
Assistant Professor, School of Management
Sir Padampat Singhania University, Udaipur-Chittorgarh Rd, Bhatewar, Rajasthan 313601
neetim01@gmail.com

Abstract

New technologies are rapidly altering the character of security issues on a global level, opening up a whole new world of new opportunities and threats at the same time. AI, info-security, biotechnology, and other autonomous systems have put strong tools for improving the security, faster and sophisticated identification of risks, and or of threats in national as well as in international contexts. These technologies have redefined intelligence collection, borders, watch, and protect, and cyber security where states/organisations have been in a position to strategize on proactive measures to security. At the same time, the growth of the technological environment accelerates the rate of growth of different risks and threats. The case of lethal autonomous weapon systems AI autonomous weapons pose certain ethical concerns such as the aspect of losing control to the software, thus having higher tendencies of initiating higher levels of conflict situations. In the same way, developments in cybersecurity responding to threats can be used to create stronger online protection, yet it has also increase the risks and possibilities of such cybercrimes such as attacks, data theft, and cyber warfare involving government intending on disrupting major establishments. Within the biotechnology domain we foresee applications of genetic engineering and synthetic biology for medical application, but these involve bio security threats such as bio terrorism and genetic data abuse. The article focused on exploring the positive effects and threat that technological advancement brings to security in the global world. This calls for enhanced and inclusive global policies, norms, and cooperation system that can well cater intertwined issues with technology ever changing and growing innovation. Through these challenges' active

management through governance, transparency and cooperation, global security stakeholders can effectively unleash technology's advantages, while at the same time managing its corollary risks.

Keywords: Global security, Artificial intelligence, cyber security, biotechnology, autonomous systems, security threats, policy adaptation, international cooperation and ethical considerations.

Introduction

The 21st century is characterized in unparalleled technological advancement, presenting both revolutionary advantages and dangers to global security. Innovations include artificial intelligence (AI), block chain, cybersecurity tools, and autonomous systems have profoundly transformed security policies and methods. These innovations provide novel methods to detect, forecast, and mitigate risks, although they may also create weaknesses that are increasingly exploited entities. This article examines the connection between technological innovation and global security, assessing how improvements function as both protective measures and potential threats. McCarthy's article, "Technological Innovation, National Security, and the American Way of Life," examines the complex interplay between technical advancement and national security in the framework of U.S. sociopolitical dynamics. It examined the interconnection between narratives of technical advancement and notions of national identity, security, and global influence. The author underscores the ideological framing of innovation as a fundamental principle of the "American way of life," accentuating its imagined function in maintaining national supremacy and confronting existential dangers. The study examined the historical development of this ideology, connecting its origins to Cold War necessities, when technical innovation served not only as a means of progress but also as a vital instrument in ideological and military conflicts. McCarthy demonstrates how this framing endures in modern policies and discourses, often influencing public and political endorsement for substantial expenditures in research, development, and defense technology. The author critically examined the possible dangers of this ideology, including the continuation of militarized innovation ecosystems and their effects on democratic accountability and global stability. McCarthy contests the presumption that technology advancement always enhances security, proposing instead that this dependence may intensify global disparities and vulnerabilities. The article advocates for a sophisticated comprehension of innovation and security, encouraging policymakers to reconcile technical advancement with ethical concerns, equality, and long-term stability. McCarthy emphasizes the need of redefining innovation to transcend its links with domination and power, promoting a more inclusive and sustainable strategy for addressing global concerns.

Theoretical Framework

The Security Dilemma Theory, rooted in the realist school of international relations, provides a framework for understanding how actions taken by states to increase their security can unintentionally lead to greater insecurity for all involved. The theory suggests that when a state perceives a threat, it may take measures to protect itself, such as increasing its military capabilities, forming alliances, or adopting new defensive technologies. Nonetheless, neighboring governments or prospective rivals often see these efforts as aggressive or menacing, prompting them to implement similar strategies. The outcome is a burgeoning cycle of distrust, tension, and military accumulation, notwithstanding the absence of original aggressive intentions from either side. The security dilemma was first described through John Herz in the mid-20th century and has since become a fundamental notion in international relations theory. The fundamental cause of the security challenge is the anarchic structure of the international system, whereby no central authority can ensure the security of nations. In such a system, states must depend on their strength and capabilities for survival, resulting in a scenario where each state's attempts at self-protection eventually diminish the security of all states. The security dilemma is crucial for comprehending historical arms competitions and military escalations. Despite neither party originally desiring open conflict, the security problem sustained a lengthy state of tension and generated an arms race that lasted for decades. In the modern context, advancements in missile defense systems, cyber capabilities, and artificial intelligence (AI) have added new complexities to the security dilemma, as states invest in progressively sophisticated technologies to secure an advantage or parity with potential adversaries. The security problem in technology innovation has become more intricate and significant. In contrast to conventional weapon systems, innovations like artificial intelligence, cyber capabilities, and autonomous weaponry may alter the equilibrium of power among states as well as between state and non-state entities. The advancement of cyber defense systems may compel adversaries to enhance their cyber offence capabilities. Autonomous weapons, including drones and autonomous combat vehicles, elicit comparable apprehensions, as countries compete to be the first to use these technologies, afraid that any delay may jeopardize their security. A significant concern about the

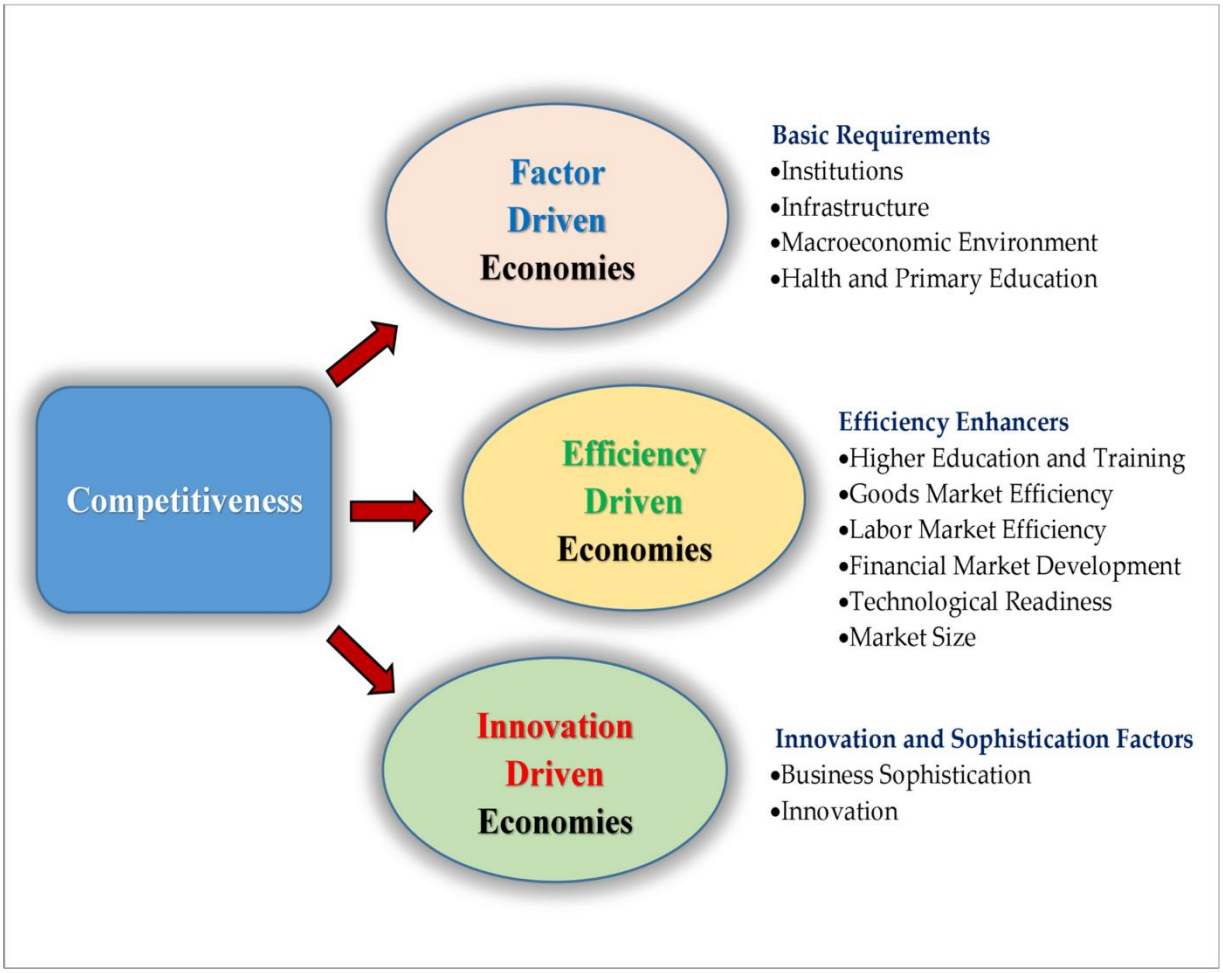
security conundrum in relation to new technology is the possibility of mistake. As nations use more sophisticated technology in their security measures, the likelihood of misinterpreting another state's intentions grows. The use of AI-driven surveillance technologies may be seen as a protective strategy by one nation, while regarded as an infringement on privacy and sovereignty by another. This uncertainty hampers conventional diplomatic discussions and increases the likelihood of inadvertent escalation, as governments may feel obligated to react to perceived threats with their own security measures. The Security Dilemma Theory is a significant framework for comprehending modern global security issues, especially when emerging technologies transform state interactions and competition. The approach emphasizes the significance of transparency, communication, and weapons control agreements to alleviate the dangers of heightened tensions. By understanding the intricacies of the security issue, nations may design methods that reconcile self-defense with collaborative security, seeking to avoid escalating cycles of fear and animosity.

Technological Determinism Theory

Technological Determinism Theory is a notion in sociology and the philosophy of technology that posits technology as a fundamental catalyst of social transformation. This theory posits that technology breakthroughs profoundly influence social structures, cultural values, and human behaviour, hence shaping historical trajectories and deciding societal consequences. The thesis posits that technology adheres to a distinct developmental trajectory, often autonomous from human purpose or societal influences, necessitating societal adaptation to these changes. The roots of technological determinism can be traced back to scholars like Karl Marx, who argued that the tools and technologies of production influence social relations and structures. Later thinkers, such as Thorstein Veblen and Marshall McLuhan, expanded on this idea, with McLuhan famously stating that “the medium is the message,” emphasizing how communication technologies like television and the internet shape human interaction and cultural norms. More contemporary proponents see technological determinism as applicable to fields such as information technology, artificial intelligence, biotechnology, and cybernetics. Technological determinism exists in two primary forms: hard determinism and soft determinism. Hard determinists view technology as the sole force that dictates societal change, often suggesting that humans have little to no control over its development. They argue that technology follows an inevitable path of progress, which society must accept and adapt to. The development of the internet and smartphones has redefined communication, commerce, and even social relationships, fundamentally altering the way people interact and access information. Soft determinism, on the other hand, takes a more balanced approach. It acknowledges the significant influence of technology on society but also considers human agency, arguing that social, political, and economic forces shape and moderate technological adoption. Soft determinists believe that while technology guides social change, people and institutions still play a role in choosing how technology is integrated and regulated. In the realm of global security, technological determinism posits that innovations in technology like artificial intelligence, robots, and cybersecurity influence the dynamics of international conflict and collaboration. The evolution of cybersecurity protocols has transformed security from physical defense to digital defense, establishing a new arena in cyberspace. Autonomous drones and AI-driven surveillance technologies have transformed combat, intelligence collection, and individual privacy. Technological determinism posits that these advances will persist in influencing global security policies and tactics, often determining international relations and geopolitical crises. Although technological determinism elucidates the influence of technology on society, it has been criticized for neglecting the significance of human agency and decision-making. Critics contend that technology is influenced by cultural, political, and economic considerations, and that civilizations may choose the degree to which they adopt or restrict new technologies. Furthermore, technical determinism may sometimes engender a feeling of fatalism, whereby society perceives itself as unable to influence or regulate technological advancement. In summary, Technological Determinism Theory provides a framework for comprehending the impact of technology on social change, often serving as a catalyst for alterations in behaviour, attitudes, and institutions. The hypothesis is especially pertinent now, since fast progress in AI, biotechnology, and digital technologies persistently transforms societies and international relations. Although technological determinism emphasizes the significant influence of innovation, it is crucial to counterbalance this viewpoint by acknowledging the agency of people, society, and governments in creating and guiding the future role of technology.

Figure: 01

Sustainable Technology in High-Income Economies: The Role of Innovation

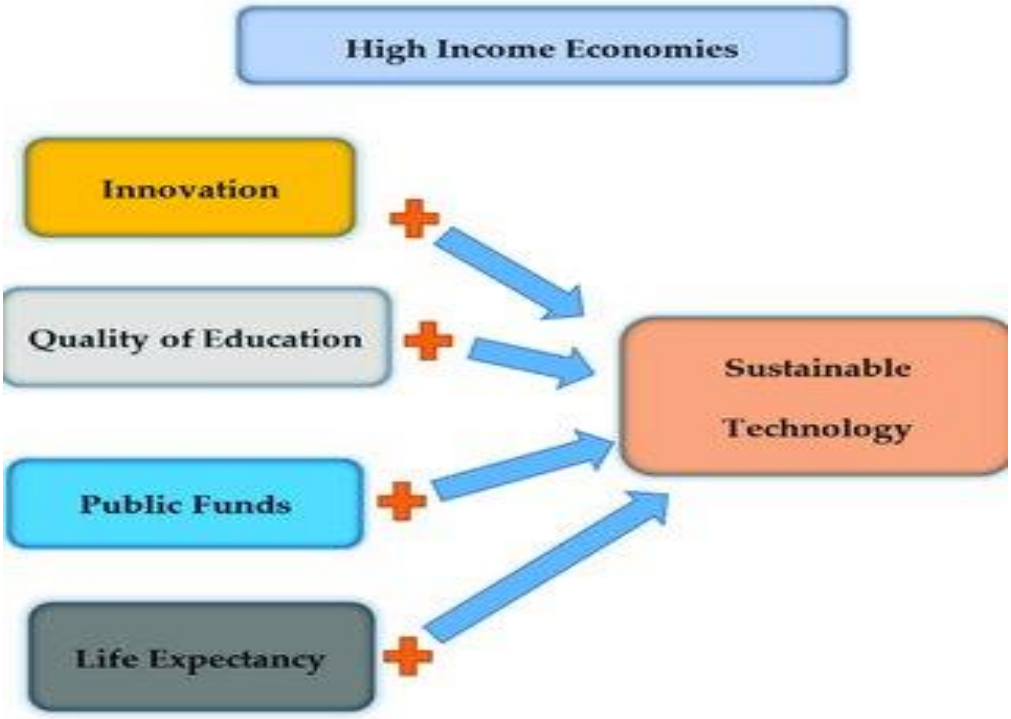


International security policies are adapting to technological changes.

As technology breakthroughs swiftly transform the security environment, international security policies are adjusting to address the emerging difficulties presented by new technologies. The emergence of artificial intelligence (AI), cybersecurity threats, autonomous systems, and biotechnology has compelled governments, intergovernmental organisations, and multinational coalitions to revise and enhance existing policies to maintain a safe and stable global environment. These adjustments seek to confront growing risks and to develop norms and ethical principles that encourage the proper use of new technology while upholding human rights and sovereignty. Cybersecurity is a significant emphasis in international security policy. As cyber threats become more complex, nations are acknowledging the need for comprehensive cybersecurity frameworks to safeguard key infrastructure, secure data, and prevent cyber-attacks. Nations are implementing cyber defense policies, creating specialized cybersecurity organisations, and improving information-sharing protocols to safeguard against state-sponsored and criminal cyber-attacks. The European Union's General Data Protection Regulation (GDPR) is a policy designed to safeguard personal data and tackle privacy issues in the context of rapid digitalization, influencing global data management practices. Moreover, programs such as NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE) provide foundations for collaborative cyber defense, promoting cooperation among member nations in cybersecurity research, training, and policy formulation. These activities underscore the global effort to establish unified cybersecurity policy in response to escalating threats to digital infrastructure. The article analyses the urgent difficulties confronting the contemporary international security system amid increasing global uncertainty. They emphasize how geopolitical transformations, technological progress, and intricate interdependencies

among states redefine the conventional concept of security. Their study focusses on the interaction between increasing multipolarity and diminishing faith in traditional international institutions, which have found it challenging to adjust to the requirements of a swiftly evolving global environment. The writers address concerns like cyber warfare, the militarization of space, and the weaponization of emerging technologies such as artificial intelligence and biotechnology. These trends, they contend, beyond national bounds, necessitating collaborative worldwide measures. They highlight the destabilizing impacts of economic inequalities, climate change, and rivalry for resources, which intensify global tensions and obstruct the development of cooperative security frameworks. The study proposed creative tools for international governance to resolve these concerns. They emphasize the need for changes in international organisations such as the United Nations to improve their ability to address hybrid threats. The article underscores the significance of diplomacy, transparency, and collective responsibility among nations to cultivate a more robust and fair international security framework.

Figure: 02



Literature review and research Agenda

Roco, (2008) explores the potential for global governance in managing converging technologies, particularly at the intersection of nanotechnology, biotechnology, information technology, and cognitive science (NBIC). He posits that these technologies hold transformative power to address global challenges, including healthcare, energy, and environmental sustainability, but also carry risks such as ethical dilemmas, societal disruptions, and geopolitical imbalances. The research advocates for proactive governance frameworks to mitigate risks while maximizing societal benefits. The study highlighted the importance of fostering international collaboration, ethical guidelines, and public participation in decision-making processes. The article emphasizes the need for interdisciplinary research and education to better understand and manage NBIC convergence. The study discusses policy recommendations, including the establishment of global norms, transparent regulatory frameworks, and mechanisms for technology assessment and foresight. He underscores the urgency of addressing inequalities in technology access and development to prevent the exacerbation of global divides..

Research Background

Historically, security and technology have been interconnected, with technological advancements often leading to shifts in power dynamics. Nuclear technology, for example, drastically altered the balance of power. Today, AI and machine learning are seen as equally transformative, with nations and non-state actors actively exploring their implications for security. From quantum computing's potential to crack encryption to biotechnology's ability to modify genes, the current trajectory of technological progress is creating opportunities and challenges that require comprehensive understanding and management.

Statement of the Problem

Technological advancements provide great levers through which to improve security, although at the same time, they pose new and increasingly serious threats that are not well understood. This research seeks to explore these risks, in an attempt to understand the implications of failure to address the risks that accompany new technologies. With regard to the multifaceted nature of the role of technology in the contemporary processes in the global security landscape, this study is designed to help avoid one-sided and reckless attitude towards innovations and security. The nature of AI, cybersecurity, and biotechnology is trendy and holds great potential to deliver substantial value addition across industries, but it has a darker facet too possible threats and weaknesses. They are in a position to develop new security risks, ethical issues, and external consequences to societies, economies, and world peace.. Here's an exploration of the unique risks and vulnerabilities associated with each:

Artificial Intelligence (AI)

i. Autonomy and Control: The growing deployment of AI in autonomous systems, such as drones and self-driving vehicles, raises concerns about the loss of human oversight. If AI systems make errors or misinterpret commands, the outcomes could be disastrous. This risk is heightened in military applications, where autonomous weapons could potentially act outside human intention, leading to unintended escalation in conflict zones.
ii. Privacy and Surveillance: AI enables large-scale data collection and analysis, enabling surveillance capabilities that can infringe on privacy rights. Government or corporate surveillance using AI for facial recognition and behavioral analysis has raised concerns over civil liberties, particularly in authoritarian regimes where such tools may be used to suppress dissent.
iii. Cyber Vulnerabilities: As AI integrates into various systems, it becomes a new target for cyber-attacks. Adversarial attacks, where malicious actors feed incorrect information to AI systems, can lead to faulty decisions in critical areas like healthcare or finance. The risk of hackers manipulating AI systems highlights a need for stronger defenses against data poisoning and model theft.

2. Cybersecurity

i. Cyber Warfare and State-Sponsored Attacks: Nations increasingly invest in cyber capabilities for both defense and offense, which has led to a rise in state-sponsored cyber-attacks. These attacks can target infrastructure, disrupt economies, or gather sensitive information, creating an atmosphere of persistent threat that could potentially destabilize global relations.
ii. Financial Risks: Ransomware assaults, in which thieves encrypt critical data and demand a ransom for its release, have increased markedly. These assaults aim at several sectors, including healthcare systems and municipal services, resulting in significant financial and operational disturbances.
iii. oT Vulnerabilities: The expansion of Internet of Things (IoT) devices, including smart household appliances and industrial sensors, has established an extensive network deficient in stringent security protocols. Numerous IoT devices exhibit susceptibility to hacking, establishing entry points that hackers may use to infiltrate bigger networks, possibly resulting in data breaches or the disruption of critical services.
iv. Data Privacy and Identity Theft: With vast amounts of personal data stored online, there is an increased risk of identity theft and privacy breaches. Cybersecurity challenges related to data storage and sharing leave personal information vulnerable to exploitation, often with severe consequences for individuals and organizations alike.

3. Biotechnology

i. Genetic Engineering and Bioethics: Biotechnology advances, especially in gene editing technologies like CRISPR, bring both opportunity and ethical dilemmas. Genetic modifications in humans, animals, or plants may offer cures or enhancements but also pose moral questions. In particular, germline editing in humans introduces concerns about unintended genetic consequences, designer babies, and potential harm to future generations.
ii. Biosecurity Threats and Bioterrorism: The increasing accessibility of genetic engineering tools raises the risk of biosecurity threats. Malicious actors could potentially create harmful pathogens or modify existing ones to enhance virulence or evade treatments, posing a risk of bioterrorism. This potential for misuse requires heightened oversight and strict biosecurity measures to prevent the creation or release of dangerous biological agents.
iii. Loss of Biodiversity: Biotechnology in agriculture, such as genetically modified organisms (GMOs), offers benefits like higher yields and pest resistance but may impact biodiversity. Modified crops can disrupt ecosystems, reduce genetic diversity, and potentially make plants or animals more vulnerable to new diseases, threatening ecological balance.
iv. Data Privacy in Genetics: With the growth of genetic testing and personalized medicine, vast amounts of genetic data are stored in digital formats, raising privacy concerns. Unauthorized access to genetic information could be misused by employers, insurers, or governments, leading to discrimination based on genetic predispositions or medical histories.

Research Objectives

1. To analyze the benefits of key technological innovations for improving global security.
2. To examine the risks and vulnerabilities introduced by advancements in AI, cyber security, and biotechnology.
3. To investigate how international security policies are adapting to technological changes.
4. To identify strategies for mitigating risks associated with emerging technologies.
5. To recommend policies that balance technological advancement with ethical considerations and security needs.

Descriptive Statistics of Perception about Technological innovations

Statements have been used to measure their level of opinion towards technological innovations. The level of opinion is measured using 5 point Likert scale and each statement is compared using the mean shown in the following table.

Table 1
Perception towards Technological innovations- Descriptive Statistics

Statement	Mean	Std. Deviation
Autonomy and Control	2.43	0.651
Bias and Discrimination	2.39	0.769
Data Privacy in Genetics	2.52	0.019
Biosecurity Threats and Bioterrorism	3.10	1.097
Genetic Engineering and Bioethics	3.22	0.380
IoT Vulnerabilities	2.76	1.369
Financial Risks	3.06	1.013
Cyber Warfare and State-Sponsored Attacks	2.41	1.109
Privacy and Surveillance	3.65	1.291

The result of the descriptive statistics shows that the mean values of all the statements of the 5 point Likert scale are between 2.41 to 3.65. It shows that the opinions about the statements are above the normal level. Autonomy and Control: The rapid advancement of technologies, especially in AI and genetics, raises concerns about autonomy. Individuals and communities may lose control over their data, decisions, or bodies as automation and centralized systems expand. Ensuring fair policies and transparent governance is essential to balance innovation with respect for personal and collective freedom. Bias and Discrimination: Algorithmic and systemic biases exacerbate discrimination in AI and genetic applications. Unequal access to these technologies may deepen existing societal inequalities. Addressing this requires careful auditing of systems, inclusive datasets, and ethical guidelines to ensure fair outcomes that represent diverse populations without perpetuating harmful stereotypes or disparities. Data Privacy in Genetics: Genetic data holds immense personal and societal value but poses risks of misuse. Unauthorized access could lead to privacy violations, insurance discrimination, or unethical research. Strong data protection laws and encryption technologies are essential to secure genetic information while allowing for advancements in personalized medicine and research. Biosecurity Threats and Bioterrorism: The dual-use nature of biotechnology poses biosecurity challenges. Engineered pathogens could be weaponized for bioterrorism, threatening global health and security. Robust international collaboration, early-warning systems, and stringent oversight of genetic research are crucial to mitigating these threats and ensuring responsible use of biotechnological innovations. Genetic Engineering and Bioethics: Genetic engineering enables groundbreaking possibilities but raises ethical dilemmas. Editing human embryos, creating designer organisms, or altering ecosystems can have unintended consequences. Striking a balance between innovation and ethical responsibility requires public engagement, strict regulations, and consensus on acceptable practices to prevent misuse and ecological harm. IoT Vulnerabilities: The Internet of Things (IoT) connects billions of devices, yet many lack robust security. This makes IoT systems susceptible to hacking, data breaches, and systemic failures. Strengthening security protocols, updating firmware, and enforcing compliance standards are critical to safeguarding interconnected systems from exploitation and ensuring user safety. Financial Risks: Technological advancements, especially in AI and block chain, impact financial systems, but also increase risks like fraud, market manipulation, and systemic vulnerabilities. Transparent regulatory frameworks, real-time monitoring, and secure infrastructure are essential to prevent crises and foster trust in digital financial ecosystems. Cyber Warfare and State-Sponsored Attacks: Nation-states increasingly engage in cyber warfare to disrupt critical infrastructure, steal sensitive data, and undermine adversaries. These attacks pose significant geopolitical risks. Strengthening cybersecurity defenses, fostering international norms, and improving deterrence measures are essential to counter such threats and ensure global stability. Privacy and Surveillance: Modern technologies enable unprecedented surveillance capabilities, often infringing on individual privacy. Governments and corporations may misuse data for control, eroding trust. Establishing robust privacy laws, promoting transparency, and advocating for ethical tech design are crucial to protecting personal freedoms and ensuring accountability in surveillance.

Discussion

AI as such has brought issues that have required fresh policy measures because the technology has implications for military, intelligence and law enforcement systems. For AI to be sustainable, safe and productive, worldwide organizations such as the United Nation have resorted to engaging in deliberations aimed at formulation of AI steering policies globally. As this field develops, these policies are intended to reflect the security needs of nation states alongside the stability of the world, traceability, and explain ability in AI. International security policies are quickly adjusting to new technologies too, for instance in the field of biotechnology, especially in genetic engineering, and synthetic biology. For the misuse of genetic technology for destructive purposes, including bioterrorism, international organizations are in the process of enhancing bio-safety. Since 1975 biotechnology has been promoted as a tool for normative cooperation and for the development of norms against the weaponization of biotechnology and the Biological Weapons Convention has become one of the key forums for the creation of conventions to monitor the biotechnology breakthroughs that might be dangerous. Ever major advancements have taken place in the biotechnology sector, countries have sought to enhance domestic bio-security measures that would protect against local proliferation of dangerous biological agents or dual-use enabling technologies. Such international policy adaptations are indicative of a general trend toward preventive and cooperative strategies concerning risk management connected with new technologies. The development of integrated standards for countries is a difficult process because every country has different goals, the level of predominant technologies, and even the general approach to regulation. Subsequently, there is not only legislative work but also discussion, the strengthening of relations in the framework of international cooperation, and the creation of instances and mechanisms for continuous assessments

of technology and ethical control at the international level. It is evident that by setting these yields in cooperation with other countries, it will be easy for all the countries to establish best practices, higher level of transparency and universal effective measures that will solve the problems that come from this influential technology thus, having a safer globe for all the nations.

Conclusion

Technological advancement as a concept forms the annals of the world's security profile in that it provides security as well as a threat. The identified results underscore the demands for collective global management, code of ethics, and policies that respond to challenges in ways that do not hinder creativity. It is only through a proactive approach to engagement with the stakeholders across the sectors, the primary focus should be placed on the ethical aspects of operations and promotion of the strengthened cooperation in the international level, that a secure future could be provided. With AI, cybersecurity, and biotechnology being just some of the industry trends, these technologies are an opportunity for development but contain high risks as well. These advancement have brought some weaknesses that need to be well managed, different sectors aggregated and ethical control. Appropriate measures of protections, responsible, and responsible ethical standard and international collaborations will, therefore, remain imperative narratives in managing these technologies and harnessing the full potential benefits of the technologies while minimizing the risks the technologies possess.

Reference

1. Adey, B. Anderson, Anticipating emergencies: Technologies of preparedness and the matter of security. Security Dialogue 43, 99-117
2. Burgess, J. P., Reniers, G., Ponnet, K., Hardyns, W., & Smit, W. (2018). Socially Responsible Innovation in Security.
3. Finnemore, Ethical dilemmas in cyberspace. Ethics & International Affairs 32, 457-462 (2018)
4. Fjäder, C. (2022). Emerging and disruptive technologies and security: considering trade-offs between new opportunities and emerging risks. In Disruption, Ideation and Innovation for Defence and Security (pp. 51-75). Cham: Springer International Publishing.
5. International Studies Quarterly, 47(4), 511-531.
6. Izmailov, Y., & Yegorova, I. (2024). Global challenges to modern international security system. Economics and technical engineering, 2(1), 22-30.
7. Mayer, M. Acuto, The global governance of large technical systems. Millennium –Journal of International Studies 43, 660-683 (2015)
8. McCarthy, D. R. (2021). Imagining the security of innovation: technological innovation, national security, and the American way of life. Critical Studies on Security, 9(3), 196-211.
9. Modarress, B., & Ansari, A. (2007). The Economic, Technological, and National Security Risks of Offshore Outsourcing. Journal of Global Business Issues, 1(2).
10. Roco, M. C. (2008). Possibilities for global governance of converging technologies. Journal of nanoparticle research, 10, 11-29.
11. Rychnovska, Governing dual-use knowledge: From the politics of responsible science to the ethicalization of security. Security Dialogue 47, 310-328 (2016)
12. Rychnovska, R. Braun, Socially responsible innovation in security: Critical reflections. Critical Policy Studies 13, 366-368 (2019)
13. Swain, A. (2012). Understanding emerging security challenges: threats and opportunities. Routledge.
14. Tsukahara, Strengthening disaster risk governance to manage disaster risk: Output of the global forum on science and technology for disaster resilience 2017. Journal of Disaster Research 13, 1177-1180 (2018)
15. Williams, M. C. (2003, Dec). Words, Images, Enemies: Securitization and International Politics.