EMERGING TECHNOLOGIES AND THEIR IMPACT ON GLOBAL SECURITY AND POWER DYNAMICS

Brig. Prof. Dr. Muhammad Amin SI (M)
Ex-VC
Baluchistan University of Engineering & Technology
Khuzdar – Pakistan
momin.alamin62@gmail.com

Abstract

This abstract focuses on developments in biotechnology, artificial intelligence, cyber capabilities, and space exploration as it examines the transformational influence of new technologies on global power dynamics and security. These advancements are the result of the digital revolution, which is propelled by the gathering and analysis of enormous volumes of data and offers potential social and financial advantages. Artificial intelligence is recognised as being integrated into a number of fields, most notably national security, with applications spanning from cybersecurity to defence and diplomacy.

The paper highlights the way the digital sphere is changing international security and how cyberattacks provide new difficulties that call for a reassessment of established power structures. Protecting sensitive data, vital infrastructure, and stable finances all depend heavily on cybersecurity. The abstract emphasises how cybersecurity shapes international diplomatic relations and geopolitical dynamics. In addition, it explores issues related to cybersecurity in the digital world, such as ransomware attacks, supply chain vulnerabilities, Internet of Things security, compliance, and data privacy. In order to mitigate cyber dangers, it is emphasised how important disaster recovery, incident response, security design, and data exchange are.

The paper examines the geopolitical ramifications of renewable energy and predicts a reduction in the political and economic sway of petrostates. It covers the effects on energy independence, the global struggle for raw materials necessary for renewable technologies, and the geopolitical power shift resulting from decentralised energy generation. Potential geopolitical disputes over transition-critical minerals and the role of some countries in regulating their supply are predicted in the article.

Finally highlights the necessity of strategic planning and future scenario analysis in light of the swift advancements in technology, shifting geopolitics, and societal shifts. To effectively traverse a changing global landscape, firms and governments must acknowledge unpredictability, assess the influence of developing technology, and incorporate geopolitical issues into continuous strategic planning.

Keywords: Technology, Global Security, Strategic Planning, Geopolitics, Diplomatic Relations

Introduction

Recent years have seen a dramatic shift in the power dynamics and global security scene due to the fast growth of innovative technology, which has presented previously unheard-of opportunities and problems for governments worldwide. This abstract investigates the complex effects of new technologies on the geopolitical scene, looking at how developments in fields like biotechnology, artificial intelligence, cyber capabilities, and space exploration have altered our understanding of security and power (Bonaci, T., Michael, K., Rivas, P., Robertson, L. J.,& Zimmer, M.,2022).

Multiple fields are seeing significant technological advancements, including biotechnology, nanotechnology, space technology, artificial intelligence (AI), robotics, information and communications technology (ICT), and quantum computing, to name a few. Artificial intelligence (AI) is particularly notable in robotics and machine learning. It is anticipated that these discoveries will cause significant disruptions and fundamental changes in the way civilizations operate.

The digital revolution that began over forty years ago is the driving force behind the technical advancements under consideration. The collection, processing, and analysis of massive amounts of data coming from the information sciences is at the core of these developments, which have ramifications for many other fields of study and development. These developments are expected to yield substantial societal and economic advantages as well as improved productivity in a variety of industries (Buzan, B. 1991).

Intelligence has several direct uses that are pertinent to national security, both domestically and internationally. "The business plans of the next 10,000 startups are easy to forecast: Take X and add AI," observes Kevin Kelly, regarding the private sector. Similar to this, artificial intelligence has a wide range of uses in national security (Onderco, M., & Zutt, M. 2021). Examples in the fields of cybersecurity, information security, statecraft in the economy and finance, homeland security, defence, intelligence, diplomacy, and development are given below. This isn't meant to be an exhaustive list of every use of AI in various domains. Instead, these are just meant to serve as instructive examples to assist individuals working in the national security field in starting to consider potential applications of this rapidly developing technology.

Cyber Security & International Security

The way that international security and security itself are evolving is greatly influenced by the digital world. Numerous writers stress the requirement that one establish and comprehend cyber principles correctly. The theories of intimidation and power preservation face significant challenges from the emerging cyber component of international affairs. Cyber attacks are

becoming more frequent, dangerous, and unstable. It is not possible to use intimidation ideas and tactics developed and used during the Cold War in cyberspace. Numerous scientists are attempting to comprehend how the internet revolution is affecting international relations. Additionally, authorities have cooperated in some ways, particularly about crime and the creation of CERTs "Computer Emergency Response Teams" (Johnson, J. 2017).

Protecting critical facilities is among the most important ways that cybersecurity advances international security. Digital systems that are networked play a major role in critical industries, including energy, transportation, and healthcare. A cybersecurity compromise may have disastrous effects, impairing public safety and upsetting vital services. Nations can guarantee the robustness of their fundamental systems and preserve the stability of their communities by safeguarding these vital infrastructures against cyberattacks (Hawk, C., & Kaushiva, A. 2014).

Furthermore, cybersecurity is essential for safeguarding sensitive private and public-sector data. Secret information on defence plans, diplomatic ties, and national security is kept by governments. Unauthorised access to this kind of data might have dangerous repercussions, including jeopardising national security and escalating geopolitical tensions. In a similar vein, people trust digital platforms with enormous quantities of personal data, including financial and medical records. This sensitive data is protected by cybersecurity, which also stops identity theft, financial fraud, and other cybercrimes that may have a significant negative influence on people around the world.

Cybersecurity is essential to maintaining financial stability and advancing global commerce in the economic sphere. Trade agreements, market activities, and financial transactions are all carried out over linked networks as economies grow more digitally advanced. Cyberattacks that target financial institutions or obstruct trade routes may have a domino effect that impacts international markets and causes economic downturns. Strong cybersecurity defences are necessary to guard against intellectual property theft, which might reduce a country's ability to compete on the international stage, promote economic growth, and preserve the integrity of financial institutions (Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. 2012).

Furthermore, national defence policies incorporate cybersecurity as a key element. Cyberwarfare is becoming a part of traditional warfare, with countries creating advanced cybercapabilities to obtain a tactical edge. Cyberattacks can be used to breach intelligence networks, interfere with communications, and destroy an enemy's military infrastructure. For a country to remain secure and to ward off possible enemies, it must be able to protect against such cyberthreats (Johnson, J. 2017).

Cybersecurity has emerged as a critical element influencing geopolitical dynamics and diplomatic exchanges in the field of international relations. Cyberwarfare, cyberespionage, and state-sponsored cyberattacks have all become instruments in the toolbox of states looking to project

power internationally. Assigning blame for cyberattacks and creating agreements and conventions to regulate the internet have grown to be essential components of global diplomacy.

Cyber Security Challenges in the Digital Age

The digital era has yielded unparalleled prospects and progressions; nonetheless, it has also presented an array of cybersecurity predicaments. Cybercriminals' strategies change along with technology (Buzan, B. 1991).

Attacks Using Ransomware: Hackers are now able to obtain user data more easily and prevent users from accessing it until a ransom is paid. Although we frequently witness ransomware attacks in movies, the IT community is most familiar with them (Reshmi, T. R. 2021). Additionally, Microsoft recently connected the data theft assault using the clop ransomware, which exploits zero vulnerabilities. Ransomware attacks are important for all users, but they are especially important for organisations whose routine operations depend on access to data. Nonetheless, even when the ransom is paid, the perpetrators of most ransomware attacks attempt to extract additional money rather than provide the data.

Vulnerabilities in the Supply Chain: Engineering systems frequently depend on a complicated web of vendors and suppliers. Every link in the supply chain presents a possible area of vulnerability. Companies must perform due diligence, evaluate the security procedures of their suppliers, and set up contractual requirements for cybersecurity (Onderco, M., & Zutt, M. 2021). Reducing risks can be achieved by routinely checking and inspecting suppliers.

Security of the Internet of Things (IoT): As IoT devices become more prevalent in framework design, it is essential to ensure their security. IoT devices often lack resilience to misuse due to weak default configurations, no firmware updates, and insufficient encryption. Strong authentication, encryption, and monitoring systems are essential for IoT devices to prevent unwanted access and any security breaches.

Compliance and Data Privacy: Sensitive data, such as personally identifiable information (PII), proprietary designs, and intellectual property, is frequently handled by engineering systems. Ensuring data privacy and adhering to relevant laws, such as GDPR or HIPAA, is crucial. Sensitive data can be safeguarded by access limits, encryption, frequent data backups, and privacy impact assessments (Kemmerer, R. A. 2003, May).

Disaster Recovery and Incident Response: Security breaches can still occur even with precautions taken. Strong policies with clear guidelines for identifying, preventing, and recovering from cyberattacks should be in place. These plans, together with information reinforcement and recovery components, need to be routinely tested and updated in order to reduce downtime and guarantee a speedy reconstruction of system performance.

Security Design: It is critical to include security from the outset when creating frameworks. Security needs are taken into account at every level of system development and implementation when using a "security by design" approach. Taking the lead in thorough security assessments and including encryption, access controls, and regular security testing may assist in identifying and mitigating vulnerabilities early on (Kemmerer, R. A. 2003, May).

Data sharing: Interaction between personnel from businesses, universities, and governmental bodies is essential when it comes to cybersecurity. Organisations may improve their security by being informed about new threats, vulnerabilities, and best practices through knowledge sharing. Collaborating with cybersecurity specialists, exchanging anonymized incident data, and taking part in industry forums may all contribute to a more robust engineering environment (Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. 2012).

Renewable Energy and Geopolitical Implications

The global energy system is undergoing fundamental changes that will have far-reaching geopolitical ramifications and impact practically every nation. The last two centuries' geopolitical landscape was moulded by fossil fuels. The ability to halt energy exports gave political influence to "petrostates," or countries whose economies primarily rely on the exploitation and export of natural gas or oil (Dodds, K. 2005). Export earnings also allowed these countries to stifle or pay off domestic opposition as well as that of other countries.

As renewable energy sources proliferate, petrostates' political and economic clout will progressively wane. This implies that countries such as the Gulf States and Russia may no longer be considered major players in the geopolitics of energy. Internal instability might result from this, possibly posing threats to entire areas. Countries like Sudan, Nigeria, and Chad may already be experiencing "shock decarbonisation" as a result of their major export, oil, seeing a sharp decline in revenue, making it impossible for their governments to maintain precarious political agreements.

Experts anticipate that at least three key changes will lead to the emergence of new conflict lines in the absence of strong global governance systems. First, switching from carbon to renewable energy also necessitates switching between various power sources. Secondly, governance structures that are closely linked to certain energy technologies will shape the future. Third, the need for transition-critical minerals to generate renewable energy on a global scale will increase and push newly formed nations into the centre of geopolitical rivalry (Tunsjø, Ø. 2011).

Geopolitical Power Shift

The ability to cut off supply of petrol and oil dominated geopolitics in the 20th century because fossil resources were concentrated in certain geographic areas. Members of OPEC (Organisation of Petroleum Exporting Countries) had the power to raise oil prices and send the economies of several industrialised nations into serious crisis in 1973 with only one decision.

In 2006, Russia could halt the gas supply to Ukraine by turning a handle, which would have immediate effects on Central and Eastern Europe. This source of power may become less prevalent as renewable energy becomes more prevalent. increased reliance on renewable energy sources. Because wind and solar energy are gathered in a decentralised manner, they are less effective as political weapons of mass destruction. Rather, power outages might evolve into a new instrument of foreign politics, and cyberattacks might become a global menace to vital energy infrastructure. A cyberattack on the Ukrainian power infrastructure in 2015 knocked down energy for 25,000 000 people in the country. (Tunsjø, Ø.2011).

Small-scale cyber sabotage is expected to become a major aspect of energy geopolitics as utilities all over the world move towards digitization, renewable energy sources, and intelligent solutions. The cyberattacks on major geopolitical actors like the US, China, Iran, and India show that big governments may also be targeted. The power instruments to disrupt and control energy are becoming more sophisticated and dispersed in the future geopolitics of energy, along with energy generation and transmission (Barichella, A. 2018).

Energy Independence

Different governing arrangements are made possible by different energy technologies. High on the geopolitical agenda of the 20th century were efforts to ensure a steady and cheap supply of carbon energy. These efforts included interventions, weapons agreements, and the formation of specialised international organisations like OPEC and the International Energy Agency (IEA). In addition, "energy statecraft," or government intervention and centralised forms of control, was necessary due to the extensive and expensive technical apparatus required to extract, process, and transport carbon energy. In contrast, smaller harvesting and storing systems that are not dependent on centralised energy networks can provide renewable energy. There are significant political and economic ramifications for this (Vakulchuk, R., Overland, I., & Scholten, D. 2020).

Due to subnational control over energy supply, exemplified by community energy networks and energy cooperatives, small-scale distributed energy generation reduces the strategic vulnerability of highly networked and digitalized systems. Thus, local and regional energy independence is a potential benefit of decentralised power generation. On the other hand, this may give local towns more authority and reduce the tax income received by national governments. By making governments more self-sufficient in energy, it also lessens geopolitical rivalry. This might change political structures and coalitions that rely on fossil fuels, such as OPEC (Goldthau, A., Westphal, K., Bazilian, M., & Bradshaw, M. 2019).

On the other hand, governments that rely on hybrid systems that offer more flexibility and self-sufficiency may be more vulnerable to international warfare than those that rely on energy monopolists. If the EU hadn't been dependent on Russian gas, it may have adopted a more assertive approach to the Ukrainian crisis.

However, because energy systems will continue to be hybrid, the foreseeable future is probably going to be a geopolitical mixed bag. Fossil fuels will continue to hold their strategic positions alongside the development of more renewable energy sources, and there will be a growth in the construction of large, centralised power-generating units like nuclear power plants and hydroelectric dam projects (Onderco, M., & Zutt, M. 2021)

Global Race for Raw Materials

Hydrocarbons served as the material foundation for energy geopolitics throughout the carbon age. New raw resources are at the centre of energy geopolitics with the move to renewable energy sources. The geopolitical constellation will change as a result of the mineral supply chains that are necessary to produce green technology.

Many see the green transition as a chance to move away from the shady politics of ensuring oil supplies, which drove a large portion of geopolitics in the 20th century. However, a worldwide scramble to secure a continuous supply of non-renewable minerals is necessary for the massive amounts of minerals required by renewable energy technology (Dodds, K. 2005).

Transition-critical minerals such as copper, cobalt, lithium, and so-called rare earth elements are expected to see exponential growth in demand as advanced nations develop electric cars, solar power plants, wind turbines, and energy storage and distribution networks.

In a post-carbon society, the person who manages the supply of these minerals will have political clout. Their geographic dispersion is quickly becoming a crucial geopolitical hub. The International Energy Agency (IEA), the European Union (EU), and others warn that political power may be exploited to manipulate the availability of minerals, endangering the sustainability of the green transition (Handke, S. 2018).

Although there are plenty of transition-critical minerals, most countries are either unable to mine them commercially due to tight domestic environmental and social rules or lack the technology to process them. Lithium, copper, and rare earth mining are very energy- and water-intensive processes that have significant negative environmental effects.

Currently, essential components for green technology come from a small number of nations that are prepared to pay the social and environmental costs—such as China, Myanmar, and the

Democratic Republic of the Congo—often with weak or authoritarian administrations. They have the potential to become the OPEC of the post-carbon future if they can convert their wealth of transition-critical minerals into political influence.

In fact, the Democratic Republic of the Congo "is going to become the Persian Gulf of the 21st century," according to the former US Assistant Secretary of State for African Affairs. Congo and other transition-critical mineral-producing nations, however, may potentially follow Nigeria's example and become victims of the "oil curse" of the post-carbon age, where their resource riches fuel underdevelopment, clandestine intrusions, and civil unrest (Bleischwitz, R., & Perincek, R. 2017).

Future Scenarios and Strategic Planning

It has never been more important for organisations to engage in thorough future scenario analysis and strategy planning in light of the constantly changing global landscape that is characterised by fast technical breakthroughs, geopolitical upheavals, and sociological transformations. Businesses, governments, and other organisations may proactively negotiate uncertainty and seize new possibilities by projecting prospective futures. This proactive strategy entails imagining realistic situations, comprehending their ramifications, and developing plans of action to prosper in a changing setting.

Understanding that there is always some degree of uncertainty in the future is essential to developing future scenario plans. It is becoming harder and harder to forecast the future with full confidence as geopolitical conflicts and the rapid advancement of technology shape international relations. Organisations may, however, generate a variety of realistic scenarios that aid in their readiness for various eventualities by recognising patterns and causes.

Future-focused strategic planning necessitates a multifaceted strategy. Businesses need to evaluate how new developments in technology, population trends, climate change, and regulations will affect their sector. Companies may create strategies that not only reduce risks but also put them in a position to benefit from new trends by recognising these factors. A manufacturing organisation, for example, can investigate adoption scenarios of automation and artificial intelligence, taking into account the potential ways in which these technologies could transform the sector.

A recent example of the value of thorough future scenario preparation is the COVID-19 pandemic. Companies that had prepared for international interruptions with backup plans were better able to handle the unexpected difficulties that the epidemic presented. Disruptions in the supply chain, changes in customer behaviour, and remote work were critical factors that companies needed to account for in their strategic planning.

The continuous advancements in artificial intelligence, blockchain, and the Internet of Things (IoT) present both opportunities and difficulties in the field of technology. Businesses need to evaluate how emerging technologies could challenge current business models and open up new avenues for creativity. For example, the healthcare sector may investigate scenarios in which telemedicine and AI-driven diagnostics become commonplace, transforming patient care and operational effectiveness.

Future scenario planning also has to take geopolitical factors into account. Businesses and governments must be ready for the effects on trade, security, and regulatory environments as the balance of power changes and new alliances form. Trade disputes, regional wars, and changes in global governance may have a substantial influence on multinational enterprises and necessitate the need for strategic adaptation (Reshmi, T. R. 2021).

Future-focused strategic planning is a continuous process rather than a one-time endeavour. Companies need to review their assumptions frequently, keep an eye out for changes in the outside world, and modify their plans as necessary. By utilising an adaptable strategy, organisations may remain ahead of the curve and convert possible obstacles into chances for expansion and creativity.

Conclusion

In conclusion, a new age of global power dynamics and security considerations has been ushered in by the dramatic shifts brought about by advances in biotechnology, artificial intelligence, cyber capabilities, and space exploration. In addition to offering previously unheard-of chances for societal and economic growth, the digital revolution—driven by the gathering and analysis of enormous volumes of data—has also brought up difficult problems that call for a reassessment of preexisting power structures.

Artificial intelligence has become an essential component of modern strategic thinking in several fields, most notably national security. In this regard, cybersecurity is essential to protecting sensitive data, vital infrastructure, and international financial stability. The dynamic nature of cyber threats, encompassing supply chain weaknesses, ransomware attacks, and security risks related to the Internet of Things, emphasises the necessity of strong disaster recovery, incident response, security architecture, and improved data sharing protocols.

Moreover, the conventional landscape dominated by petroleum is changing due to the geopolitical implications of the shift to renewable energy. There are new problems brought about by the declining political and economic dominance of fossil fuel-dependent nations, such as possible conflicts over transition-critical minerals and a shift in the power structure of decentralised energy generation. International politics must take into account the geopolitical tension created by the worldwide competition for rare earth elements and lithium, two raw commodities that are crucial to renewable technology.

The paper emphasises the importance of future scenario planning and strategy planning in managing the quickly changing global environment. It emphasises the need for governments and organisations to proactively adapt to new issues by highlighting the unpredictable nature of technological breakthroughs, geopolitical upheavals, and sociological changes. A contemporary illustration of the importance of careful planning for potential future scenarios is the COVID-19 pandemic, which highlights the necessity for adaptability and resilience in the face of unforeseen setbacks.

In short, going ahead, strategic planning must be done continuously and with flexibility. Organisations may position themselves to not only manage risks but also take advantage of new possibilities for development and innovation by comprehending the complex effects of technical advancements, geopolitical changes, and societal upheavals. In a world where everything is always changing, the capacity to manage the complex interactions between these elements will be essential to maintaining stability, security, and prosperity.

References

Barichella, A. (2018). Cybersecurity in the energy sector: A comparative analysis between Europe and the United States. Ifri: Etudes de l'Ifri.

Bleischwitz, R., & Perincek, R. (2017). Raw Materials and International Relations. Sicherheit und Frieden (S+ F)/Security and Peace, 129-133

Bonaci, T., Michael, K., Rivas, P., Robertson, L. J.,& Zimmer, M. (2022). Emerging technologies, evolving threats: Next-generation security challenges. IEEE Transactions on Technology and Society, 3(3), 155-162.

Buzan, B. (1991). New patterns of global security in the twenty-first century. International affairs, 67(3), 431-451.

Dodds, K. (2005). Global geopolitics: A critical introduction. New York: Routledge.

Gates, L. P. (2010). Strategic planning with critical success factors and future scenarios: An integrated strategic planning framework. Software Engineering Institute, 11, 67.

Goldthau, A., Westphal, K., Bazilian, M., & Bradshaw, M. (2019). Model and manage the changing geopolitics of energy. Nature, 569, 29–31.

Handke, S. (2018). Renewables and the core of the energy union: How the pentalateral forum facilitates the energy transition in western Europe. In D. Scholten (Ed.), The geopolitics of renewables (pp. 277–303). Cham: Springer Nature.

Hansen, A. M., & Larsen, S. V. (2014). Use of scenarios and strategic planning to explore an uncertain future in Greenland. Regional environmental change, 14, 1575-1585.

Hawk, C., & Kaushiva, A. (2014). Cybersecurity and the smarter grid. Electr J, 27(8), 84–95.

Johnson, J. (2017). Roadmap for photovoltaic cyber security. Sandia National Laboratories. Report No.: SAND2017-13262.

Kemmerer, R. A. (2003, May). Cybersecurity. In 25th International Conference on Software Engineering, 2003. Proceedings. (pp. 705-715). IEEE.

Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. (2012). Cybersecurity and privacy issues in smart grids. IEEE Commun Surv Tut, 14(4), 981–997.

Onderco, M., & Zutt, M. (2021). Emerging technology and nuclear security: What does the wisdom of the crowd tell us?. Contemporary Security Policy, 42(3), 286-311.

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. International Journal of Information Management Data Insights, 1(2), 100013.

Tunsjø, Ø. (2011). Geopolitical shifts, great power relations and Norway's foreign policy. Cooperation and Conflict, 46(1), 60-77.

Vakulchuk, R., Overland, I., & Scholten, D. (2020). Renewable energy and geopolitics: A review. Renewable and sustainable energy reviews, 122, 109547.