*Pakistan Journal of Humanities & Social Sciences Research*
*Volume No. 07, Issue No. 02 (December, 2024)*

ISSN (P): 2663-9211 (E): 2663-922X
DOI: https://doi.org/10.37605/pjhssr.v7i2.3

Date of Submission: 19st October, 2024
Date of Acceptance: 20th November, 2024
Date of Publication: December, 2024

# Dynamics of Software and Strategic National Security: A Futuristic Perspective

**Dr. Muhammad Zia-ur-Rehman**

## Abstract

*This study focuses on a comprehensive approach to National Security, encompassing the protection of a National Sovereignty, territorial integrity, and citizenry from internal and external threats. This multifaceted concept includes intelligence gathering, military defence, counterterrorism, cybersecurity, and related measures. The research addresses National Security in its broadest sense, incorporating the safeguarding of political stability, economic progress, and promotion of international interests. The research highlights the role of government institutions and agencies responsible for defence, as well as the vital functions of the intelligence community in ensuring National Security. In the rapidly evolving 21st century, where technological advancements are transforming the security landscape, countries are adapting and progressing at an unprecedented pace. Consequently, this study emphasizes the significance of software in various aspects of National Security, including Military Security (MS), Cyber Security (CS), Environmental Security (EnS), Economic Security (EcS), Border Security (BS), Intelligence Security (IS), Infrastructure Security (InfS), and Human Security (HS). The study anticipates a future where National Security will increasingly rely on the strength, reliability, and validity of software, effectively becoming a "war of software." The study provides theoretical and practical implications for future researchers and policymakers, offering valuable insights for the development of effective National Security strategies.*

***Keywords:*** *National Security, war of software, artificial intelligence, future perspective, Government*

## Introduction

Amidst of a rapidly evolving global landscape, catalysed by the advent of artificial intelligence, the international arena is undergoing a profound transformation, yielding diverse trajectories and possibilities (Smith et al., 2021). This accelerated pace of change is, in turn, reconfiguring the dynamics of national security. The traditional notion of national security has become increasingly obsolete, necessitating a paradigmatic shift towards a more comprehensive understanding of national security as a multifaceted concept that encompasses the protection of a nation and its citizens from a wide range of internal and external threats. This expanded conceptualization of national security transcends conventional military

defence, intelligence gathering, and counterterrorism measures, incorporating the critical domain of cybersecurity.
The imperative nature of national security lies in its capacity to ensure the stability, sovereignty, and well-being of nations, safeguarding the lives and security of their citizens. Furthermore, national security is indispensable for preserving a country's political interests, promoting economic progress, and contributing to regional and global stability and security (Chen et al., 2019). It is evident enough that software plays a critical role in emerging latest technology, enabling machines like computers and other devices to perform a wide range of complex tasks. Software allows users to interact with the device, manage and organize data, and perform specific functions including the basic like word processing, to higher level like data analysis, and communication.

The rapidly evolving global landscape, characterized by the emergence of artificial intelligence and technological advancements, has transformed the dynamics of national security. The traditional notion of national security, focused solely on military defence and territorial integrity, is no longer sufficient to address the complex and multifaceted threats of the 21st century. The imperative of national security extends beyond mere protection of citizens and territory, encompassing the preservation of political stability, economic progress, and promotion of regional and global stability.

Despite the growing recognition of the need for a comprehensive approach to national security (Tzenios, 2023), existing research has primarily focused on isolated aspects of national security, such as military defence or cybersecurity (Akhtar, 2023). There is a dearth of research that holistically examines the intersection of technological advancements, artificial intelligence, and national security (Adewusi, 2024). Furthermore, the role of software in national security remains understudied, with limited research exploring its implications for national security strategies and policies (Horowitz. 2024). This study aims to address this research gap by investigating the impact of software on national security and exploring the future perspectives of national security in the context of technological advancements.

The study focuses on the critical role played by software in the arena of security. It also enables the development of various applications which can be used in favour or in against security, such as games, social media, and e-commerce platforms. Side by side, the study highlights numerous aspects as they enable automation of many tasks and processes, making them more efficient and costeffective.it is of more significance when it comes to national security related to Pakistan, as the country is facing multitude of challenges and issues both internal factors and from external actors.
The study focuses on:

- To investigate the dual-use nature of software and its potential applications in both Favor of and against security

- To examine the role of software in automating tasks and processes related to national security
- To identify the benefits and challenges of using software in enhancing national security in Pakistan
- To analyse the impact of software on internal and external security threats faced by Pakistan
- To provide recommendations for leveraging software to promote national security in Pakistan

**Literature Review**

software plays essential role in the field of machine learning and artificial intelligence, unleashing extreme power to computer systems and allowing them to make decisions and perform tasks that were once considered only possible by humans. Let's have a quick look at some uses and abuses of software.

*Uses and Abuses of Software*

Software is employed in a wide range of fields and industries for multiple purposes such as spreadsheet programs, word processors, and management tools are employed to increase and efficiency and productivity in organizations. Software, such as emails, messaging platforms, and video conferencing tools are brought in to facilitate effective communication and collaboration among not only individuals but also teams, as many software such as music players, video games, and streaming services can be used for many other purposes including entertainment and leisure. Similarly, there exist other software relevant to inventory management, accounting, and customer relationship management systems (CRMSs) which are highly effective and are used to manage and analyse organizational operations. On the other hand, software also provides big assistance in education and healthcare industries, such as learning management systems (LMS) s used in majority of the organizations, educational games, and interactive whiteboards, are used to enhance the learning experience for students, and for healthcare, electronic medical records, patient monitoring systems and medical imaging are very useful to improve the effectiveness and delivery of healthcare services to save millions of lives. Furthermore, Machine Learning and Artificial Intelligence have augmented software and enhanced its strength, where it is used to train learning models for machines and build AI-augmented applications such as natural language processing, image recognition, and many more. Now people I the world have established Internet of Things, where software is not only used to connect, control, and monitor a wide range of devices but also employed for systems on the Internet of Things (IoT) ecosystem. And in this situation, we cannot ignore robotics, where software is used to program, control, and monitor the functioning and behaviour of robots, including their sensors, movement, and all actions.

While on one hand, when software can be used for many beneficial purposes, on other hand, it can also be abused in numerous ways. In this context, Malware are malicious software, including Trojan horses, viruses, and ransomware, which can be highly dangerous and can be used to disrupt normal operations, steal personal information and damage computer systems. Similarly, software can be used by

hackers to get unauthorized access to networks, and computer systems, and steal sensitive information, and disrupt whole system and thus operations too. Spams are also the software that can be used to send unwanted and unsolicited emails and that can clog up anybody's or organizational email inboxes and be a nuisance to all the users. World has experienced as agents try using Phishing, where again software can be used negatively to create fake emails and websites that look real and legitimate, to trick users into giving away their very personal information including passwords, credit card numbers and alike. Similarly, we are not unaware of Spyware, where software can be used to check, monitor and collect personal information about users without their consent an even without their knowledge. Furthermore, Adware can be used to send and deliver unwanted popups, advertisements, and other forms of intrusive marketing for negative purposes.

And if a software is not strong enough, and can have vulnerabilities and flaws, that can be easily exploited by attackers to intrude and gain unauthorized access and perform malicious actions to get what the set target. This leads us to cyberstalking, where software can be used by cyberstalks to threaten, harass, and even monitor someone online. In addition to this, cyberbullying is established where software can be used to intimidate, bully, or harass someone who is online (Chen et al., 2016). Therefore, it is imperative to be aware of such abuses of software and take appropriate measures to protect against them, such as using software against software like anti-malware and anti-virus and, being cautious about opening the links by clicking on links and opening some attachments from unknown sources and keeping software up to date with the latest security patches.

*Software and National Security*

It is universally acknowledged fact that software has been used for various purposes, and it plays a critical role in national security (Hoadley et al., 2019), as it is used to protect against cyber threats and support various intelligence oriented and military operations. some of the essential software related to national security include Cyber defence which can be used, where software is used to protect institutions, government and military computer systems and networks from cyber-attacks, such as malware, viruses, and hacking attempts. similarly, intelligence gathering software can be employed to gather, analyse, and disseminate essential intelligence information, such as imagery intelligence (IMINT), signals intelligence (SIGINT) and Command and control-oriented software (CCS) can be used to support the command and control of military operations, including logistics systems, communication systems, and decisionmaking strategies.

When it comes to fighting force, weapons play vital role, software assists a lot in weaponry, as the weapon systems software are available and are employed to operate and control various weapon systems, such as missiles, drones, and even aircrafts. This leads to in cyber warfare, where software can be used as a weapon itself and as in cyber warfare, it can be employed to disrupt and destroy military systems and critical infrastructure, and to monitor and track. Surveillance software can be used to track and monitor individuals and groups, not only domestically but also internationally, thus preventing terrorist attacks, espionage and other criminal activities. Likewise, other software like Encryption software is progressively used that can be employed to encrypt data and communications,

to protect them from unauthorized surveillance and access. Additionally, to get better understanding for decision making strategically, we need analysis of big data, so data analytics software can be used to analyse large amounts of data to identify and track trends, patterns, and connections that can be used to support human intelligence. It is to say that the use of software in national security also raises other concerns like ethical and legal ones, as it can be used to restrict civil liberties, as it can invade people's privacy, and can perform activities that may be seen as unjust and illegal. Institutions, Governments and security services need to ensure that their use of software adheres to the regulations and laws that protect citizens' rights and prevent it from being used for illegal or unethical activities (Smith et al., 2018).

*Challenges to the National Security of Pakistan*

Pakistan faces various challenges, and they are getting complex in nature. National security in the context of Pakistan is a complex and multi-faceted phenomenon, as it is a country that is facing a range of external as well as internal challenges. Some of the key threats to Pakistan's national security may include insurgency, terrorism, boarder security issues, cybersecurity, India Pakistan relations, and economic security. Pakistan is the country that has been affected by terrorism the most for many years, as there are various domestic and international terrorist agencies and groups operating across its borders. The government of Pakistan has been taking actions to counter terrorism and anti-extremism through intelligence gathering, military operations, and even through law enforcement efforts. In some part of the country, challenges are enormous, as insurgent groups in Baluchistan and the formally Federally Administered Tribal Areas (FATA) have been active for decades. They have been a source of violence and instability in the region. The government of Pakistan has been taking action to counter the insurgency through both development programs and through military operations. Naturally, Pakistan is a country having long and porous border with Afghanistan, that has been affected by war and then used by various terrorist groups. The government has been taking some serious actions to improve border security and recently like the construction of fences across the border, increasing security patrolling, and also deployment of additional troops there. On the other hand, even trying its best, Pakistan's relations with its neighbour India have long been adverse, due to major flashpoint of Kashmir, which is occupied by India illegally, and due to many other issues. Based on Pakistani sincere and positive efforts, the two countries have engaged in several attacks, however not succeeded and various conflicts emerge. And the potential for further escalation remains a significant concern for Pakistan's national security. Various issues include, like Pakistan's government and its private sector have been targeted by cyber-attacks from neighbouring country and even through its non-state actors. The enemies try to harm Pakistan through multifarious propaganda. The government of Pakistan has been taking various action to improve its system through cybersecurity and through the development of regulations, policies, and enhancing cyber defence agencies but on the other hand, the country's economy is facing big challenges over the last few years, they became severe, which has led to unemployment, increased poverty, and that decreased in the standard of living for many of its citizens. In order to address such challenges, government of Pakistan has been

planning and trying to take a multi-pronged approach, including diplomatic efforts, military operations, economic development, and even social welfare programs for its citizens. Furthermore, the country also tries its best to cooperate with its neighbouring countries. It has tried to establish better relationship with international organizations for improving its national security, however it is to say that in order to ensure national security, that is not enough. The country needs to establish extensive awareness and proper ethical usage of software, which is the need of the face various sorts of challenges.

*Pakistan's National Security and use of Software*

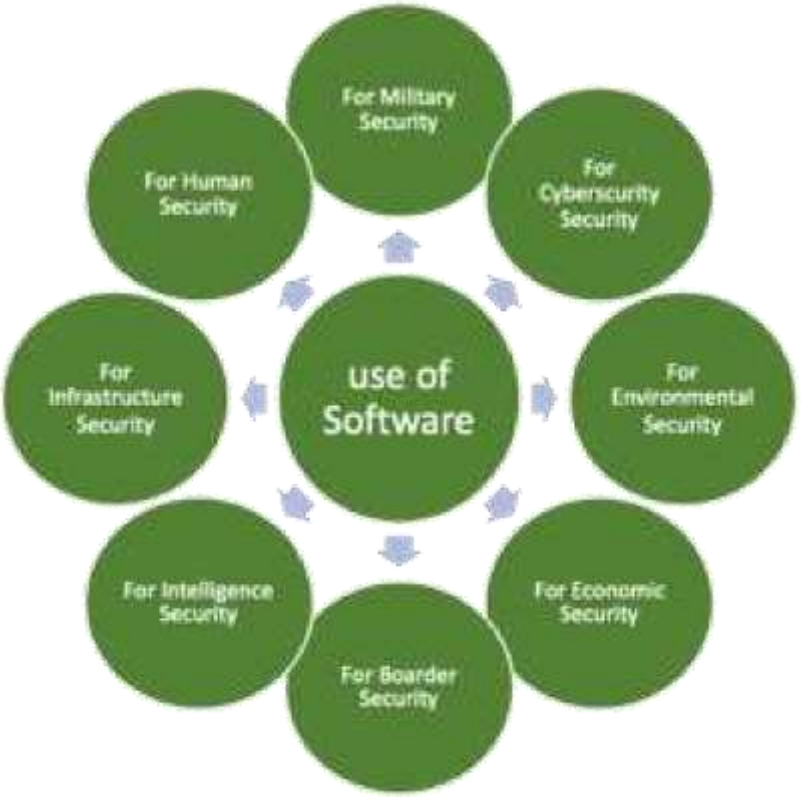
As mentioned earlier, Pakistan needs to keep its country and nation secure through any means including military security, which means protecting the nation from external military threats, through cyber security which is needed for protecting the nation's information and digital infrastructure from cyber-attacks. Then it also needs to ensure economic security, which is needed for not only protecting the nation's economic interests but also establishing stability. Similarly, the country needs to ensure sustainable nature through environmental security (Lee et al., 2020) which is needed for protecting the country and countrymen from environmental threats and natural disasters. Then we see that the nation is suffering from poverty and hunger as well, therefore food security is necessary which needs to be ensured that the countrymen have availability and access to the safe and nutritious food. Likewise, the country is also having energy issues, and energy security is the need of the hour and by ensuring the availability and access to affordable and reliable energy sources is imperative. And securing the country from external physical threats, the country needs border security, which means protecting the nation's borders from trace passing, smuggling and illegal immigration. Furthermore, Intelligence security is also essential, as it is based on gathering information and analysing information to prevent potential threats to the country and its countrymen. The country has few good infrastructures in form of motorways metro, water dams, national facilities, orange train, airports, and other constructions, for this infrastructure security is required, which deals with protecting the nation's critical infrastructure, such as transportation systems and even power grids.

**Methodology and Analysis**

This research employs a conceptual analysis approach, building on existing literature to develop a futuristic framework for enhancing national security in Pakistan. Using a qualitative methodology, we conducted a comprehensive content analysis of secondary data, identifying key themes and patterns. Our analysis reveals that human security is a critical component of national security, emphasizing the need to protect citizens from physical harm and ensure access to basic needs.

Based on our in-depth review of existing literature and expert opinions, we propose a strategic framework for promoting national security in Pakistan. This framework prioritizes the protection and well-being of citizens, ensuring their safety and access to basic needs such as food, water, shelter, healthcare, and

education. It also addresses internal and external security threats, including terrorism, cyber-attacks, and geopolitical tensions, while leveraging software and technology to enhance security measures and improve efficiency. Furthermore, our framework adopts a holistic approach to national security, integrating human security, economic security, and environmental security. Our proposed framework offers a futuristic approach to national security in Pakistan, addressing




the complex security challenges facing the country while prioritizing the protection and well-being of its citizens.

Strategic Proposed Conceptual Framework

*Use of Software for Military Security*

For any country, the strength of military has become essential for not only survival but also to safeguard its countryman. It has also become very important to face any aggression from outside. Therefore, countries all over the world specifically the developed nations try to adopt and inculcate various strategies to strengthen their military secrets services. In military security, the use of software has been tremendously increased as Software can be used in various ways to enhance military security. One of the essential elements of military security is information gathering, and for Intelligence gathering and analysis: software Assist a lot as it can be used to collect and analyse data from various sources, including satellite imagery, for providing the military leaders with critical information as well as the potential threats to avoid. In military, the commandand-control system is crucial which is used to manage and coordinate personnel, through communication and operations. The coordination, operations, communication and even controlling is done through command-and-control system. And the system needs to be efficient, effective and synergistic, for this it is going to be heavily relying on software. Therefore, sooner in future the hold command and control system of the military security would be relying on software. Additionally, even in military operations unmanned aerial vehicles (UAVs) are managed through software. Then the whole military system is established including command and control system, there comes cyber security which ensures that the military systems, the networks, and command and control system or protected from cyber-attacks and intrusion. Likewise, for enhancing the skills, and abilities to have better military security, trainings and simulation or necessary elements, for which software can be used instead of real dying next betterments. That safeguards the lives and reduces risks a lot by developing scenarios, military trainings, logistics and supply chain in virtual environment.

*Findings*

Software helps a lot in establishing and planning military operations including supplies, personnel, tracking equipment, and ensuring effectiveness. Furthermore, autonomous weapon system software can also Be employed to manage and control weapons system without any manual intervention, including drones' operations and guided missiles based on artificial intelligence-controlled weaponry in military security.

*Use of software for Cybersecurity*

The use of software in cyber security cannot be undermined as we all know that Cybersecurity software is used to protect networks computer systems, and data from disclosure, unauthorized access, use, modification, disruption, or destruction. There could be various examples of cybersecurity software including firewalls, antivirus programs, intrusion detection system, encryption software and intrusion prevention system. such software and system in cybersecurity are the tools that can strengthen the security and prevent cyber-attacks like hacking

attempts from enemies or agencies or groups, protecting systems from malware infections. similarly, such cybersecurity software also helps in responding and detecting the security breaches effectively, thus providing security to the institutions, the countrymen and the country

*Use of software for Economic security*

Another important security for any nation and country is called economic security. It refers to the ability of people, organizations, and nations to maintain financial stability and ensure the basic needs of life. there are various ways to safeguard economic security and ensure it (Johnson et al., 2021). Here, also software can play critical role in obtaining economic security through providing systems and tools for facilitating communication, managing and analysing financial data, and commerce, and even automating various financial Procedures and processes. One essential use of software in economic security is in field of financial management, where for example, accounting software, allows organizations to track their expenses and income, generate financial statements, and even plan for future progress and growth. On the other hand, there exist personal finance software, that allows individuals to track their investments, manage their budgets, and plan for retirement and life after. Such software provides valuable insights into financial performance, by identifying trends, making informed decisions, and taking steps to improve financial stability. Similarly, another essential usage of software in economic security is related to e-commerce, as we can see online payment platforms and online shopping that allow individuals and businesses and to buy and sell goods and provide services, supporting trade, business and economic growth. In this way, E-commerce software also enables secure and efficient online transactions, through the risk of financial losses and fraud. Furthermore, there are software for logistics and supply chain management that can optimize the flow of information related to goods and services, and that leads to improved efficiency, cost savings, and overall economic stability (Rovner et al., 2018). In addition, software has been increasingly used in financial services, such as banking and investment. Automated systems, such as online banking and trading platforms, have made it easier for individuals and businesses to access financial services, manage their accounts, and make transactions. These tools have also improved transparency and security in the financial system, reducing the risk of fraud and other financial crimes.

*Findings*

Therefore, software plays a vital role in achieving economic security by providing tools for financial management, facilitating trade and commerce, and automating various financial processes. These tools help individuals, businesses, and nations to maintain financial stability and support economic growth. Therefore, to ensure economic security, it's crucial to learn and remain linked with latest software developments and usage that are reliable and secure.

*Use of software for Environmental Security*

In this modern world, the care for environment is the care for human being and society. Therefore, huge attention has been paid to safeguard and secure

environment. The use of software for environmental security can have great value as it has become increasingly important in recent times as the world is facing a growing number of environmental challenges. And environmental security actually refers to the protection of natural resources and the related ecosystems from the negative effects of human activities, including pollution, climate change and deforestation. Software plays a crucial role in dealing with such issues by providing the strategies, tools and data which can be needed to comprehend, monitor, and even manage the whole environment. One of the major uses of software in environmental security can be in the field of remote sensing, where the remote sensing technology, including drone-based mapping, and satellite imagery allows environmentalists and scientists to collect data on large areas of land and even from water efficiently. This type of data can be used to identify and detect changes in land use, or to track the spread of invasive species, and to monitor the health of the ecosystems. Furthermore, software can also be employed to analyse the data and create detailed maps and models that can be used to inform conservation and management decisions. Similarly, essential application of the software in environmental security can be in the field of modelling and monitoring where the use of software can track and also predict the effects of climate change on natural resources and on even whole ecosystems. Like, the related software can be employed to model the effects of sea level rise on coastal communities, and also it can predict the effect of changing temperatures on even vegetation patterns. Such pieces of information can be very useful in assisting governments and organizations to plan for and to respond to the impact of climate change, and even to make decisions about land use and conservation. Furthermore, software can also be used to monitor other environmental hazards and even pollution, as software can be employed to track the spread of pollutants in water, air, and even to monitor the health and security of wildlife populations. This data can be very useful to identify the sources of pollution and then relying on authentic data, to design effective management and strategies for mitigation. Even further, software can be employed to assist public engagement and awareness towards environmental security through mobile apps and online platforms which can be used to share information about efforts made for conservation, or even to provide resources to the public to learn more about environmental problems and take care of them. Likewise, other digital tools and social media can be used to mobilize actions by raising awareness about environmental security issues. In this way, one can say that software plays a crucial role in addressing the environmental challenges and its role is increasing day by day, as we face the world to address such issues.

*Findings*

From monitoring and remote sensing till modelling and public engagement, software provides various assistance and tools in understanding data, manage resources, and protect environment. As the word changes fast, technology continues to advance, and it is very likely that the usage of software for environmental security would become essential coming months and years.

*Use of software for Food Security*

When it comes to major national issues including hunger and poverty, then security of food it's essential element. Food security refers to the strategies

through which accessibility availability, and stability of a sufficient amount of safe food and nutritious need to be made ensured to meet the dietary needs of countrymen. Here, too, software again plays a vital role in ensuring food security through offering tools and technologies for tracking and managing food systems properly, starting from the whole chain from production to consumption. In this context, one of the most important methods in which a software can be employed in food security is through the systematic management of agricultural production (Brown et al., 2020). For example, the Precision agriculture software, allows farmers to optimize, and enhance crop yields by using pertinent data on soil conditions, weather, and other related factors in order to make more informed and well thought out decisions about the whole process of seeding, planting, watering, fertilizing and even harvesting. This assists and can help ensuring that there is enough food available in the country to meet the needs of the population, and that it can be produced in a proper sustainable way. Additionally, the key area where software can be used in food security is in the supply of food and distribution process. Here software-oriented systems like Inventory management systems, can allow retailers and food distributors to track and check the movement of food products throughout the supply chain process, and help to quickly respond if there emerges any change in demand. In this way, software helps to ensure that food is sufficiently available to those who need it, and also assist those who are involved in distribution, to process it in an equitable and efficient manner. Furthermore, for protection and distribution, software can be employed to handle various matters related to nutrition and food safety, as the software tools can be assistant to analyse and track incidents related to food safety. In this way risk mitigation can be done in a systematic manner. Likewise, the tracking of nutrition can be done through tracking software, which can be used to monitor the population of the country and its dietary intake. Hence providing them or customized recommendations for improving the nutrition and diets.

*Findings*

Therefore, it cannot be undermined that software in full security can play critical role and by providing technologies and tools in order to not only track but also manage the food systems, we can ensure to fulfil the needs of the countrymen with the sustainable supply, Efficiently and effectively. In this way software can be very good assistant in helping the policymakers to fight against modern nutrition and hunger by managing food security in an active equitable manner.

*Use of software for Energy Security*

Energy security refers to the steps and measures adopted to ensure the stable and reliable supply of energy including fuel, electricity and other energy sources, to fulfil the requirements of organizations, society and individuals. and if energy is properly managed and secured, then it can reduce the dependency of the country on foreign sources of energy. Side by side if the sources of energy are diversified and protected against the disruption in the energy supply including backup power generation and emergency stockpiles, this can not only benefit individuals but the whole society in general as it is the problem of the whole world. Generally, the whole world, and specifically Pakistan is facing energy crisis since long it's emancipation. Some experts are of the opinion that the country possesses ample amount of energy, however the energy wastage creates big problem for the nation. Therefore, appropriate supply and usage of energy again help the nation. Not only

energy generation is important but more important is energy security, because the whole National security and economic stability depends on energy and its security. This helps the country for disaster preparedness with efficiency and effectiveness as I know this guilty is crucial in modern society because it is critical for providing power to everything starting from home appliances, houses organizations from our businesses, transportation, industry and the whole society. Here also software can be used very efficiently in order to optimize the distribution, production, and even consumption of energy. one of the essential areas where software can be very efficiently help in energy security is strategic management of power grids, as smart power technology provides real-time not only monitoring but also controlling of generation of electricity, distribution, and responding to the demand and supply accordingly. Software can help in preventing the power will stitch and outages quickly by responding to the demand and supply. in this way the overall efficiency can be enhanced, and powered power outages can be prevented related to the grid. Another aspect where software can be employed in energy security is by using renewable energy sources where software can help optimizing the operation of solar plants, wind power and thus maximize their energy output on one hand while minimizing the reliance on the carbon emission-oriented fossil fuels.

Furthermore, software can be used to assist in managing energy storage systems, such as batteries, in order to ensure that excess of energy if generated by renewable sources can be preserved and can be made available for use as and when needed. Software can also be employed to Enhance the efficiency of energy in industrial P transportation s and in buildings, Software can help maintaining building management systems which can be a great assistant to monitor and control heating and Co lighting and energy consumption in buildings properly. Why software can also be used in managing transportation systems effectively through optimizing the roots and reducing the fuel consumption of the system. Similarly, when it comes to industry, the industrial process control systems can be employed for efficient consumption, manufacturing and production, in this way use of software in energy security is crucial to ensure that we have a sustainable and reliable energy supply. Therefore, software can be very helpful in optimizing the production, bringing efficiency in consumption and distribution of energy, and thus reducing reliance on fossil fuels. Thus, software can help improving the efficiency of energy systems by ensuring the sustainable and secure energy for future, which involves numerous methods to safeguard energy security encompassing its management, renewable energy system, smart grid software-based systems and energy trading platforms. Some examples can include as energy management software can monitor and control the consumption of energy in buildings as well as in other facilities including factories and industrial zones, by increasing efficiency and reducing energy costs. As we know that most of the infrastructure is managed by computer systems therefore software can be very useful here, as ensuring undisrupted and sustainable energy supply can protect against any cyber-attacks. renewable energy management software can be employed to enhance the renewable energy systems performance including wind, and solar which ensures that they produce as much energy as possible efficiently. Similarly, software can help stopping the wastage of energy add appropriate usage and supply of energy based on the demand, as energy trading platforms can be

established to allow the consumers and the energy producers to sell and buy in real time, thus it can help to bring balance in demand and supply and further enhance the efficiency, and reliability off the energy grid.

*Findings*

Additionally smart grid software can be employed to increase reliability and efficiency of electric grid which can enable real time monitoring and controlling of the grid. This encompasses all the parts into and integration and thus distribution of energy resources can properly managed. some of the usage of software for energy security are mentioned here but there can be many more and software can have critical role in energy security for the country and the countrymen through enhancing the process had three levels energy generation, energy distribution, and energy consumption. and they had all three levels software can be of great assistance and a tool to ensure energy security.

*Use of software for Boarder Security*

Even in this modern world of technology and advancement, security of a country's borders is crucial. Border security involves all the measures and management undertaken by the countries to not only monitor but also control the movements of goods, animals and even people across the borders. But management really needs physical patrolling, fencing, putting barriers, and surveillance technology. The other side of the coin reads about the unauthorized or illegal immigration and measures taken to check immigration process. Therefore, both aspects of border security need to be ensured as the objective of border security is to protect the country and its countrymen from any potential terrorism call mom spread of disease or any sort of threat. The security of borders is crucial for any country, because it protects the country and its nation from any potential threats do its countrymen, any threat to its resources, and any trespassing to its territorial sovereignty. There are various ways to protect and safeguard borders however the most effective way is using software for border security. Here we will discuss few of the most important software that can be used for border security. As we know that to ensure border security, it can be done through the use of surveillance technology, data analysis tools and biometric identification. It is universally acknowledged that surveillance technology is the most widely and universally employed tool for border security which includes a complete package of drones, cameras, and sensors which can not only monitor the movement of human but also record and detect the movement of vehicles across the borders. they are all software-based systems, and they can very easily and efficiently identify and detect the potential issues, thus tracking the potential threats including illegal immigration, smuggling or any other sort of activity. such software driven advanced system can be employed to detect the patterns of any suspicious activities and help identifying the potential threats. For border security, the biometric identification system is also based on software, which use fingerprints, facial recognition, behavioural characteristics, physical structure, and iris scan for identifying, recognizing, and keeping record of the individuals. Such software driven systems can be very efficient to identify the individuals at border crossing, points of entry, and at airports. They can very easily help preventing the people who are for example at terrorist watch list or those who possess criminal activity history. furthermore, biometric identification systems driven by software can also be very useful to track individuals' movement within the country, thus identifying

and tracking any potential threats. Another software could be related to data analysis tools which are critical components of border security and can be used to not only analyse the big data sent by biometric systems surveillance footage or tracked history but also analyse and generate the trends and patterns to help decision makers take actions proactively.

*Findings*

Likewise, software-based data analysis tools can be employed to track resources and their sources, for example tracking the financial transactions and identifying its origination and thus assisting in detecting money laundering or any other white-collar crimes including financial crimes. in this way software you can play key role to enhance border security through multiple ways, tools, and systems.

*Use of software for Intelligence Security*

Another very important security is related to intelligence security of a country, where intelligent security is referred to ensure and protect the information, people and assets from sabotage, breach, as espionage, and related intelligence activities that may challenge or threaten national security (Lee et al., 2017). To counter such activities, countries and their governments try to use threat analysis, and counterintelligence strategies. The use of secure communication systems and protecting the sensitive information is also necessary. Similarly planning and implementing efficient security measures which do not allow unauthorized access to information or areas or even preventing manipulation. In the field of intelligent security, software has been gaining more and more value as the technology advanced and information and its volume increased. As the volume of the data and transmission of the information has increased tremendously, the significance of the secure transmission and storing electronically also gained its value. software can be very useful at the fundamental level it can be encryption which is a process of converting unencrypted information or the plain text into encrypted information or ciphertext by employing mathematical algorithm. The role of software here is so important that it ensures that even if some data or information or intercepted by some unknown or unauthorized agency or individual, the information will not be readable without some appropriate decryption key. similarly, another use of software for intelligent security includes access controls, which are employed to restrict the excess too sensitive information based on permissions and the user's identity. In this way software makes sure that only those who are authorized can have access to sensitive information and use that. likewise for intelligent security, software can be employed for preventing prevention system and intrusion detection, where such systems are programmed to prevent and detect unauthorized access to systems or networks. This can be achieved through various methods including monitoring network traffic for detecting suspicious activities, conducting comparison of network traffic with a database of known threads and even employing machine learning algorithms to detect the unusual behaviour patterns. furthermore, software can also be very useful for intelligent security when it assists through a system called Security Information and event management (SIEM), We had such systems planned together, analyse and appropriately respond to the multisource data that is security related, In real time. In this way software helps organizations to quickly identify, detect and then respond to the security threats. Another important usage of

software for intelligent security is the use of vulnerability management systems, where such systems are planned and designed for scanning a system or network in order to identify and detect vulnerabilities and then offer various options and recommendations as remedies. in this way software can provide security to overall organizational security posture and keeps it up to date by addressing the vulnerabilities before occurrence. for example Palantir, which is a data analysis platform which can be used by law enforcement organizations and intelligence agencies for Analyzing large amount of data from multiple sources, AML is an advanced data analytics software which can be employed by intelligence and security agencies for detecting and preventing money laundering, ArcGIS is a great software, which is a geographic information system (GIS) based software that can be employed by intelligence services and organizations for mapping and analysing data in a geographic context. Similarly, Analyst's Notebook is a data visualization tool which has its usage in intelligence related organizations for analysing ad visualizing the complex data for specific purposes.

*Findings*

Then there is Signals Intelligence (SIGINT) software which can be used by intelligence agencies to detect, intercept and analyse the electronic communications including emails, phone calls, and even text messages.

Furthermore, Social media monitoring software can be employed by security agencies and intelligence related institutions to monitor the platforms of social media and detect any potential threats, and it is pertinent to mention that the mentioned software is not exhaustive and there might be other software that are used by intelligence services.

*Use of software for Infrastructure security*

for the development of any country, the infrastructure please very important role, which is referred to the organizational structures, facilities, including physical as well as structural facilities like buildings power supplies, roads rail tracks, airports and uh all such infrastructure need to let the countrymen survive and operate within our country. infrastructure can also include facilities related to functioning of the community and services including communication networks transportation systems and other public services. to build infrastructure is not an easy task and that for public purpose where government and countries not only spend a lot of financial resources but also huge amount of time. At once build and construct it their security is essential to be taken care of. Here there are various software that can be employed to safeguard infrastructure, including industrial control system security software (ICS), which is designed to protect industrial control systems including power plants and other national infrastructure. Then Disaster recovery and business continuity software (DRBCS) how's the organization to prepare and recover from power outages, natural disasters or any other hazards. Software like backup and recovery software, disaster recovery as a service (DRaaS), are used for planning purposes. Similarly, Security Information and Event Management (SIEM) software can be employed to gather, analyse and find association in log data coming from multiple sources including servers, network devices, and applications in real time.

*Findings*

Furthermore, SIEM software can be used by the organizations to respond and detect security related incidents or accidents and handle the response effectively and quickly. And vulnerability management software includes penetration testing tools and vulnerability scanners which can be off greater help in securing country' national infrastructure.

*Use of software for Human Security*

When it comes to security, the most important security is of all the securities is considered as human security which is referred to the protection of people and communities from various hazards and threats, including economic deprivation, physical violence, and even environmental degradation. Human security is a multidimensional and broad concept that embraces issues and aspects related to individuals' personal safety, getting access to essential and basic services, providing protection to human rights and serving the society. nowadays other threads are from outside or from inside, both need to be countered effectively to safeguard the people as well as the state. in this 21st century technology has become essential player for human security (Rovner et al. 2018), and one of the best ways to safeguard human security is through proper use of software. there are wide range of applications and systems that can perform basic tasks of data entry, word processing still the most complex tasks including surveillance monitoring, threat detection and even decision making. It is imperative to note that by employing software to ensure human security, it can greatly enhance effectiveness and efficiency of the existing security operations, for example it can automate various tasks including surveillance, monitoring and even detecting through video footage or any unusual activities. In this way software can help to release the other resources to be realized on other tasks, providing opportunity to the security personnel to pay attention on more essential does including emergency response, or potential threats investigation and alike. The use of software in human security and shorts are comprehensive and much more accurate big picture of the security situation in any country or in any organization, as the software can process huge amount of data accurately, quickly and thus makes it possible to identify the patterns or trends that may have been not so be easily detectable by the human eye. such human security related software can be employed to analyse data related to social media.

*Findings*

As it is a qualitative study, therefore the results are extracted in the form of findings. Software related to human security can assure prevention of cyberattacks, vulnerability and safeguarding from hacking the data, however one needs to be aware of the potential conditions Including monitoring systems for signs of breaches, security protocols, and providing security trainings too the employees. The findings show that there are numerous applications of the software in security systems, whether its human security or even at large scale national security, the role of software cannot be undermined. And with the emergence of AI and machine learning, the significance of the use of software has increased tremendously.

**Conclusion**

Conclusively, we can say that, in the rapidly evolving world of the 21st century, the dynamics and challenges ahead are increasing exponentially, and the importance of human security cannot be under-rated. In this context, software has the potential to play a vital role in ensuring the safety and well-being of individuals and communities. With the right approach, software can be leveraged to address the complex security challenges of the modern era, from cyber threats to data protection, and from artificial intelligence to the Internet of Things.

By harnessing the power of software, we can develop innovative solutions to mitigate risks, prevent threats, and respond to emergencies. Moreover, software can facilitate collaboration, information-sharing, and decision-making among stakeholders, ultimately enhancing the effectiveness of human security efforts. As the world grapples with increasingly complex security challenges, it is essential to recognize the critical role that software

**References**

Akhtar, N. (2023). Emerging Cyber Security Challenges: Implications for Iranian National Security. BTTN Journal, 2(2), 83-106.

Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. World Journal of Advanced Research and Reviews, 21(1), 2263-2275.

Bian, C. (2020). National security review of foreign investment: a comparative legal analysis of China, the United States and the European Union. Routledge.

Wang, K., Wang, Y. W., & Wang, Q. J. (2022). Will monetary policy affect energy security? Evidence from Asian countries. Journal of Asian Economics, 81, 101506.

Kang, X., Wang, M., Lin, J., & Li, X. (2022). Trends and status in resources security, ecological stability, and sustainable development research: a systematic analysis. Environmental Science and Pollution Research, 29(33), 50192-50207.

Lu, Y., Zhang, Y., Hong, Y., He, L., & Chen, Y. (2022). Experiences and lessons from Agri-Food system transformation for sustainable food security: A review of China's practices. Foods, 11(2), 137.

Smith, K. F., Goldberg, M., Rosenthal, S., Carlson, L., Chen, J., Chen, C., & Ramachandran, S. (2014). Global rise in human infectious disease outbreaks. Journal of the Royal Society Interface, 11(101), 20140950.

Chen, D., Wawrzynski, P., & Lv, Z. (2021). Cyber security in smart cities: a review of deep learning-based applications and case studies. Sustainable Cities and Society, 66, 102655.

Chen, J. A corpus-based study on China's international counterterrorism discourse (2001-2021) (Doctoral dissertation, University of Nottingham).

Hoadley, D. S., & Lucas, N. J. (2018, April). Artificial intelligence and national security.

Horowitz, M. C., & Kahn, L. (2024). Bending the Automation Bias Curve: A Study of Human and AI-Based Decision Making in National Security Contexts. International Studies Quarterly, 68(2), sqae020.

Cameron, A., & Tedds, L. M. (2021). Gender-based violence, economic security, and the potential of basic income: A discussion paper. Economic Security, and the Potential of Basic Income: A Discussion Paper (April 30, 2021).

Johnson, B. A., Kumar, P., Okano, N., Dasgupta, R., & Shivakoti, B. R. (2022). Nature-based solutions for climate change adaptation: A systematic review of systematic reviews. Nature-Based Solutions, 2, 100042.

Johnson, B. T. (2021). Sensing the Arctic: Situational awareness and the future of northern security. International Journal, 76(3), 404-426.

Al-Suqri, M. N., & Gillani, M. (2022). A comparative analysis of information and artificial intelligence toward national security. IEEE Access, 10, 64420-64434.

Zhuang, Y., Choi, Y., He, S., Leung, A. C. M., Lee, G. M., & Whinston, A. (2020). Understanding security vulnerability awareness, firm incentives, and ICT development in Pan-Asia. Journal of Management Information Systems, 37(3), 668-693.

Tennakoon, W. D. N. M. S., Janadari, M. P. N., & Wattuhewa, I. D. (2024). Environmental sustainability practices: A systematic literature review. European Journal of Sustainable Development Research, 8(3).

Seet, P. S., Klarin, A., Jones, J., Johnstone, M. N., Wilk, V., Meek, S., & O'Brien, S. (2024). Expanding Australia's defence capabilities for technological asymmetric advantage in information, cyber and space in the context of accelerating regional military modernisation: A systemic design approach.

Schild, J., & Schmidt, D. H. EU and US Foreign Economic Policy Responses to China.

Jervis, R., Gavin, F. J., Rovner, J., & Labrosse, D. N. (Eds.). (2018). Chaos in the liberal order: The Trump presidency and international politics in the twenty-first century. Columbia University Press.

Lane, H. G., Turner, L., Dunn, C. G., Hager, E. R., & Fleischhacker, S. (2020). Leveraging implementation science in the public health response to COVID-19: child food insecurity and federal nutrition assistance programs. Public health reports, 135(6), 728-736.

Rovner, J. (2025). Strategy and grand strategy in the Cold War. Adelphi Series, 65(514-515), 81-114.

Zegart, A., Rovner, J., Warner, M., Lindsay, J., Maschmeyer, L., Fischerkeller, M. P., ... & Kollars, N. A. (2023). Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest. Georgetown University Press. Rovner, J. (2018).

Biddle, S., & Zirkle, R. (1996). Technology, civil-military relations, and warfare in the developing world. The Journal of Strategic Studies, 19(2), 171-212.

Rovner, L. L. (2024). Solitary Confinement, Human Dignity, and the Eighth Amendment. U Denver Legal Studies Research Paper Forthcoming, 111.

Snow, D. M. (2019). National security. Routledge.

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. The Journal of Strategic Information Systems, 30(4), 101693.

Schmidt, J. I., Johnson, B., Huntington, H. P., & Whitney, E. (2022). A framework for assessing food-energy-water security: A FEW case studies from rural Alaska. Science of The Total Environment, 821, 153355.

Raikes, J., Smith, T. F., Baldwin, C., & Henstra, D. (2021). Linking disaster risk reduction and human development. Climate Risk Management, 32, 100291.

Johnson, J. (2021). 'Catalytic nuclear war'in the age of artificial intelligence & autonomy: Emerging military technology and escalation risk between nuclear-armed states. Journal of Strategic Studies, 1-41.

Tzenios, N. (2023). How Does Cultural Psychology Influence the Perception of National Security Threats?. Charisma University.