The Digital and Cyberspace Modernization Strategy; A Possible Strategical Roadmap to Transform Traditional Military Organizations into a Smart Military through the Emerging Information Technology

Dr Saleem Ahmed
OUC Universal College
in partnership with
Liverpool John Moores University, UK
Doha Qatar
saleem@oryxuni.com

2022 International Conference on Computer and Applications (ICCA) | 978-1-6654-5294-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCA56443.2022.10039571

Abstract— **The report provides idea about how the military organizations could be improved for using future information technology. It provides a detail knowledge about the possible strategies that could be used by the military organizations to change their traditional work process into new advance digital process. The report will discuss about the implication of the emerging technologies in Military organizations and how the organization could adapt to these changes. The emerging technologies have the power to change "the rules of the games" whether it's about balancing the military power among security actors or balancing the competition in the market among the new entrants and existing companies. Thus, it has become important for organizations to adapt to these changes.**

The report will discuss about the implementation of Artificial Intelligence, Machine Learning and Blockchains in military organization and, will also provide idea about the potential challenges that military organizations are facing in adopting them. Further it will discuss about the possible strategies that military organizations could adopt to make their employees get familiar with these new technologies and get benefitted from it.

The Unites States has made major improvement in their field of technology and the country is said to be the leader in the development of most of these technologies. The United State military has relied on the technological superiority for ensuring their dominance in conflict and also for underwriting their national security. China and Russia have also made improvement in the development of advance military technologies. Hence, going through this report will also provide knowledge about the implementation of emerging technologies in military organization of some countries and what are the things that other military organization should learn from them.

Keywords - Emerging Technology; Artificial Intelligence; Machine Learning; Digital and cyber modernization; Blockchain; smart military

I. INTRODUCTION

The research paper provides idea about how the military organizations could be improved for using future information technology and facing the cyber challenges. Over the last few years, the rate of cybercrime has increased all over the world and has become a global issue. In today's time all the companies including the military organizations are ingrained in cyberspace. All the things including personal messages between family and friends to diplomatic dispatches and, top secrets of military organizations are being created, received, transmitted and read in "1s and 0s" of computer codes. In short it could be said that cyber space touches all aspect of 21st century lifestyle, this has made cyber-attacks more frequent and deadly to disrupt the computer networks, power grids and, defensive and offensive military equipment's. The research paper will give a detail knowledge about how the military organizations could be improved so that they could fight against the cyber-attacks and use the new information technologies for betterment of the organization.

In recent years there has been a substantial improvement in technology for determining and detecting such cyber-attacks but yet there are a lot of areas were the organizations need to make enhancement and bring more advanced technologies in use. An organization needs practice and preparation to recover effectively from cyber-attacks and the main challenge to sustain cyber resilience is facing constant change in the work culture of an organization. Many Military organizations encounter changes on daily basis which include change on work process, application or the use of new technologies. Therefore, if security controls will not adjust to keep pace, the companies will have to face vulnerabilities that could expose them for month or years. The paper will discuss about strategies and techniques that could be used by Military organization to implement the use of Information technologies, Artificial Intelligence, Machine Learning and Blockchains, so that they could mitigate the risk of cyber-attacks (Reding & Eaton, 2020).

In order to provide a clear knowledge to the readers the research paper has been divided into different sections. First, there is a brief abstract that discuss about the core topic of the paper and provides a reader with a brief idea of the research topic. Then comes the introduction part, it contains authentic and relevant data related to the project topic and the research questions and research objectives are clearly defined in this section. The research paper aims at fulfilling the objectives of the paper and also provide authentic answers to the research question. Thirdly, a literature review section is developed and, in this section, information is collected from different articles and journals of various authors. The information collected from the previous research studies and articles are authentic and relevant to the research topic. Further the research paper provides detailed knowledge of the strategies and frameworks that could be used by the military organization for implementing new technologies, it provides idea of the methods and techniques that the organization could use to make their employees get familiar with the use of new technologies at workplace.

RESEARCH OBJECTIVES:

1. to determine the strategies and measures that could be used my military organization to transform traditional military organization into smart military organizations.

2. to determine the importance of use of advanced technologies in military organizations.

3. to identify the upcoming new technologies that could be use in military organization for possible change.

II. LITERATURE REVIEW

A. *Improvement and modernization of military organization for facing cyber challenges and using future information technology :*

In recent years the importance for getting prepared and recovering from cyberattacks has increased drastically. It has been found that the U.S military has made improvement in their military organization by implementing new and advanced technologies. In the year 2016, the momentum of preparing from cyberattacks was seen in the budget that was requested from White House, in that budget the former President of U.S Barack Obama asked $19 billion for building the cybersecurity, that was 35 % more than the previous year (Nurkin & Konaev, 2022). That request of cybersecurity made by U.S gives a backdrop to the government agencies to think twice about their approach towards cybersecurity. As the technologies are advancing the risk of malicious threats are increasing and it is required for federal civilian and military agencies to get prepared for cyberattacks. The ability of an agency to recover effectively from the cyber-attacks needs practice and preparation. Therefore, for facing cyberattacks military organizations are required to adopt the new and advanced technologies, but the major issue that organizations face in implementing these technologies is facing constant change. The adoption of new technologies in organization brings changes and the employees face difficulty in adjusting with such changes; thus, it has become crucial for companies to adjust with the changes and make their employees prepare to face this change (Nunes, 1999).

The organizations could rely on the military readiness model to fight against cyber-attacks, this model will help agencies build resilience from ground level and sustain those targeted resilience through perpetual change. The military readiness model assumes that in an organization change takes place in every area and adjusting training and resourcing plans according to change will help in better adjustment and acceptance. Furthermore, it has been found that in response to cyber breach in the year 2013, navy executed “Operation Rolling Tide,” a plan for removing adversary from the unclassified network of Navy and give security to the network from more penetration. The key elements of the plan include establishment of clear control and command, synchronizing defender activities and network operator, defining responsibilities and roles and developing effective communication plan externally and internally. After the cybersecurity culture took hold, the organization are required to train and educate their employees about the use of new technologies so that they get familiar to it and makes its best utilization when needed (dodcio.defense.gov, 2019).

B. *Expansion of cyber skills at military organizations:*

As software is becoming more integral part of human life, that national security experts of U.S military has recognized the need for improving their software fluency. The U.S military has understood that in order to become dominant at future battlefields they will need better knowledge of software and technology. Enhancing cyber technology has become the first priority of Biden administration and they are also focusing on improving their STEM knowledge in their national security workforce so that they get prepared for the upcoming future challenges related to technology. The Department of Defense has already identified the urgency of improving their cyber skill sets at both leadership and personnel levels. The 2018, cyber strategy of DoD believed that the organizations staffs and leaders are needed to be cyber fluent in order to understand the implications of cyber security in their decision-making process and, are also in a position to identify the opportunities that are related to cyber domain for gaining operational, strategic and tactical advantage (Ryseff, 2021)

In similar manner the Air force have decided to enhance their proficiency in digital sector by encouraging the airmen to learn the languages of computer in the same way they encouraged them earlier to learn about foreign languages. Still, just learning about this skill sets will not be the best and proper way to educate the leaders and officers in military organization to face and fight against cyber specialists. It is being discussed that both cybersecurity and software engineering are detailed and complicated studies and one need to have a deep knowledge of it if they want to fight against it effectively. Thus, just providing the leaders and employees with a few weeks course will hardly give them any detailed knowledge about cyber security and software engineering. Hence, instead of providing their existing employees with few weeks course, organization should focus on encouraging the upcoming personnel and leader learn about the technical discipline. For example, in the IT companies the product managers are provided with the responsibility of identifying customer need, and for this the manager undergoes deep research and tries to understand the needs of the customer so that they could be satisfied in the best possible way. Once, the product manager identifies the need of the customer they go to the software developer team and guide them to provide proper solution to the customer as per the customers need (Golden, 2016).

Moreover, when the organization face problem with inevitable resources and limited time, the project manager is the one who decides the most essential capabilities that could be used to deliver the product. Thus, the product manager performs the role of bridge between the rest organization and the engineers, this means they should learn to communicate properly with both the non-technical teams and the technical teams. The product managers handle multiple tasks at the same time, like at one meeting they are required to convince the engineering team to develop proper product with all the required features added, on the other side they convince compliance team to work as per the procedures and policies. Once, all this is completed the product manager is required to explain the work value to the leaderships of the organization. Therefore, having this kind of skills and knowledge will also help the officers of Military organizations on more than just attending and completing an introductory lesson on programming.

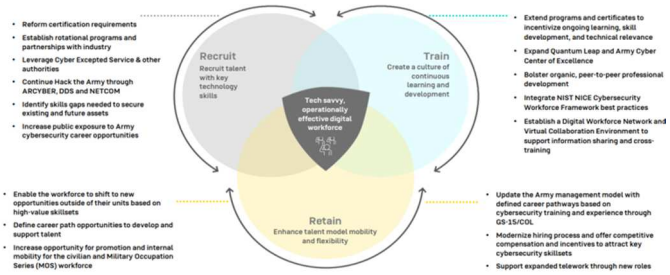


Figure 1: Building cyber workforce

Additionally, for encouraging the officers, the organization should consider some incentives. Firstly, they could develop a certification in for advancing the O5 and O4 rank to combat some specialties. Like in Navy the surface warfare officers are responsible to protect the carrier groups from the missiles and submarines of enemies, and the process of detecting and destroying such adversaries are dependent on automation and software. Therefore, the warfare officers of mid-carrier surface might be taught about these new concepts and skills. Secondly, the Department of Defense could create new opportunities for their officers by putting their skills and knowledge into practice. Thirdly they could motivate their officers in developing their product management skills at the time of disassociated tours. The military already have some of their personnel in technology companies like Amazon and Microsoft for learning more about business practices Thus the organization could enhance the prestige of such assignments by encouraging their ambitious officers to seek the opportunities out.

C. *Implementation of advance technologies in military organization:*

(i) Implementation of AI:

The implementation of new and advanced technologies in military organizations have increased and some of the developing countries like U.s Russia and China has already started implementation of hypersonic weapons, artificial intelligence, lethal autonomous weapon, quantum and biotechnology weapon and directed energy weapons. The use of this technologies has helped Russia, U.S and China to transform their traditional military operations into smart military operations. Artificial Intelligence is referred to any behaviour that is like human but is displayed by a system or machine. It has been found that the investments of DoD's in AI have increased from $ 600 million in the year 2016 to around $874 million in the year 2022, with the organization maintaining more than 685 active artificial intelligence projects. The U.S DEPARTMENT OF Défense has established joint Artificial Intelligence centre (JAIC) for coordinating more than $15 million DoD projects (Nurkin & Konaev, 2022). JAIC has undertook several National Mission Initiatives for Artificial Intelligence, which include disaster relief and humanitarian aid, business process transformation, predictive maintenance and war fighter health. Moreover, a Joint Common Foundation is also being maintained by the JAIC for a "secure cloud-based AI development and experimentation environment" this joint foundation supports fielding and testing of AI capabilities department-wide. It has been found that in the year 2021 the Deputy Secretory of Défense, Kathleen Hicks directed to establish the Chief Digital and AI office that will "serve as the successor organization to the JAIC, reporting directly to the Deputy Secretary of Defence."

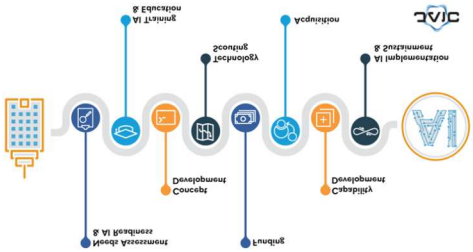
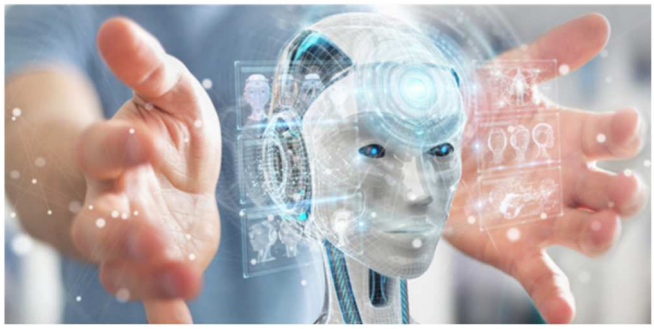


Figure 2: Adoption journey of AI in JAIC

Further the author Nunes (1999), states that, in the international market of AI China is seen to be the closest competitor of U.S in the year 2017. The recent achievements of China in the field of AI demonstrates its potentiality to realize its goal for development of AI. It has been found that China has developed facial and language recognition technologies, and they are planning to integrate this in the domestic surveillance network of the country (Nunes, 1999). Additionally, it has been found that China is developing different types of sea, land, air and undersea military vehicles, the country is also actively pursuing the swarm technologies

which could be used in adversary missile defence



interceptors. Moreover, some publications show that China is establishing an AI tools suite for their cyber operations (dni.gov, 2021).

Figure 3: Artificial Intelligence

The president of Russia Vladimir Putin said in one his statements that, "whoever becomes the leader in AI will become the ruler of the world." However, it has been found that currently in the development of AI Russia significantly lags behind China and the United States. Thus, in order to overcome the gap Russia has launched a national strategy which outlines 5-10 years benchmark to enhance the datasets, AI expertise, legal regulator systems, infrastructure and educational program. Moreover, it has been found that Russia has indicated that it will robotize 30% of its military equipment by the year 2050. The author states that Russia is conducting a thorough research on several AI applications by emphasising heavily on autonomous and semiautonomous military vehicles. Additionally, the military organization of Russia is planning to incorporate Artificial Intelligence in naval, undersea vehicle and unmanned aerial and is also focusing on the development of their swarming capabilities. The implementation of this technologies will help Russia in reducing their manpower requirements and cost and will enable the country to field more system with little personnel (Fidock, 2006).

(ii) Implementation of Hypersonic Weapons:

Hypersonic weapons are the weapons that fly at high speed of Mach 5, or could be said as the five times of the speed of sound. The hypersonic weapons are of two types mainly first is Hypersonic glide vehicles, this are basically launched from rockets before they glide to target and second is Hypersonic cruise missiles, this has high-speed engines throughout the time of their flight. (James, 2013).

It has been found from researches that China has developed the intercontinental ballistic missile- DF-41 (ICBM), that could carry nuclear hypersonic glide vehicle, as per a report of 2014 by the U.S-China Economic and Security review commission. General Terrence O' Shaughnessy, who was the commander of Northern Command of U.S confirmed the assessment in February 2020 after testifying that "China is testing a (nuclear-capable) intercontinental-range hypersonic glide vehicle, which is designed to fly at high speeds and low altitudes. complicating our ability to provide precise warning." In addition, it has been found that China has tested DF-ZF hypersonic glide vehicle approximately nine-times from 2014 and the defence officials of U.S has stated that these missiles have the capability to perform evasive maneuvers at time of flight (James, 2013).

Furthermore, it has been found that Russia is concerned for the development of hypersonic weapons as President Putin stated in the year 2018 that "the U.S is permitting constant, uncontrolled growth of the number of anti-ballistic missiles, improving their quality, and creating new missile launching areas. If we do not do something, eventually this will result in the complete devaluation of Russia's nuclear potential. Meaning that all our missiles could simply be intercepted." Thus, Russia is seeking hypersonic weapons that could maneuver their targeted approach for penetrating U.S missile defence and restore the sense of strategic stability (Sayler, 2022).

(iii) Implementation of Big Data and Advanced data Analytics:

The big and advances data analytics explains about the analytical methods that could visualize large volumes of information. The enhancement in the new communication models, internet of things, and the virtualisation of the socio-cognitive space contributes towards development of the big data. From the starting of the year 1960, the world is becoming increasing virtual and digital and in the coming next year the trend is about to increase more and will have a disruptive impact on the capabilities and alliance operations. This magnitude of this data sets become difficult to handle logistically because of the increase in the velocity, volume, visualisation, variety and velocity and this is going to present significant organizational, technical and interoperability challenges. Thus, the new communication technologies, autonomy, distributed sensors, digital twins, virtual socio-cognitive space and the development of the expanded analytical method will enhance the ability of organizations to understand the information, physical and human spaces around them. The BDAA will provide the technology for all the EDT's and will also help in the enhancement of the Military Capabilities. Moreover, the implementation of the big data analytics will drive the need and development for AI.

(iv) Implementation of Quantum technology:

The implementation of Quantum technology in an organization help in translating principles of quantum physics in technological applications. However, the use of this new technology has not yet reached maturity, but it is expected that it could hold major implication for future of military encryption, communication and sensing. It has been found that under Quantum technology other military applications could also be formed like quantum sensing, that could function to enable major enhancements in the submarine detection, rendering ocean transparent. This in turn could help to compromise survivability of sea-based nuclear deterrent of U.S. As per the Défense Science Board Task Force on implementation of the Quantum Technology assessment, three applications of the quantum technology proved the most promising for the U.S military this includes, quantum communications, quantum computing and quantum sensing. The task force thinks that the implementation of quantum sensing could enhance the ability of DoD to carry out some missions, providing timing options in environment and precision navigation where GPS is denied or degraded. Further the use of quantum computers could provide potentiality to substantial computation power of DoD for AI, signals processing and decryption, and lastly the implementation of quantum communication could enhance the networking technologies (events.afcea, 2022).

It has been found that China has prioritized their research on quantum technology in their development plans. The quantum communication and the quantum computing are the main research initiatives of China. In addition, it is being found that China is already a leader in the development of quantum technology and the year 2016 the country launched the first quantum satellite of the world to provide "global quantum encrypted communications capability." In the year 2017 China established the -first quantum-secured intercontinental video conference. Furthermore, it has been found that the development of quantum technology is Russia lags far behind of China and U.S and in December 2019, Russia announced their plan of investing $790 million in quantum research over the next 5 year. Russia also adopted a five-year Russian Quantum Technologies Roadmap (James, 2013).

D. The Implication or Outcome of emerging technologies in military organizations:

The strategic stability of and the implication of emerging technologies in military organizations are difficult to predict, but not impossible as they are going to perform as many factors, which include the interaction among the emerging technologies, the process through which the emerging technologies will be integrated concepts of operation and existing military forces, the rate of advancement in technology in both U.S and its competitor nations and the extent to which the international law and the national policies will enable their integration, use and development. Furthermore, it has been found that there are several emerging technologies that are going to impact the future character of war. The enhancement and development in technologies like big data analytics, AI, and lethal autonomous weapon could remove or diminish the requirement of human operations. This in turn will help in enhancing the efficiencies of the military organizations with potential destabilization of consequences (Snyder, et al., 2015).

Additionally, it has been found that effective interactions among these emerging technologies could also enhance the capabilities of the existing militaries with unforeseen consequences for strategic stability and warfighting. For example, if quantum computing could be paired with AI it will become enable of producing a more powerful process of Machine Learning, which will provide the potentiality to make improvements in target identification, image recognition and will also enable a more enhanced and sophisticated autonomous weapon. Likewise, AI could also be combined with the new 5G communication technologies for enabling virtual learning ad training environments or could be combined with biotechnology for enhancing robotic systems, or human cognition. However, this developments in the military organizations will require new and improved concepts of operation, tactics and strategies.

Figure 4: Autonomous technology

Furthermore, it has been found that the enhancement in the use of blockchain technologies (along with the use of quantum technologies and Artificial Intelligence enables cyber bots) will increase the ability of the Military organizations to ensure trusted data and communication storage. The finding highlights that over the coming 20 years the volume of data is going to increase, as the internet connected device are growing exponentially. It is expected that by the year 2030 approximately 500 billion data will be interconnected and handing this amount of significant data will create difficulty for the companies. Therefore, the implementation of technologies like blockchain will help the organization in handing such big amount of data and run their operations smoothly.

E. The expected and upcoming new IT technologies that could be used in military organization a possible change in military technology till 2040 :

The author states that in the coming 20 years it is expected that the four overarching characteristics will mainly define the advancement in the military technologies. This includes intelligent – this technology would exploit the integrated Artificial Intelligence, symbiotic AI -human intelligence for providing disruptive application throughout technological spectrum, and knowledge-focused analytical capabilities. Distributed- this include employing ubiquitous and decentralized large-scale sensing, computation for achieving new disruptive military effects and storage. Interconnected- this would help in exploiting network of physical and virtual domain including the networks of autonomous agents, organizations, individuals and sensors, linked with the new distributed ledger technologies and encryption methods. Digital- this includes information and physical domains for supporting novel disruptive effects and digitally blend humans. It is been expected that the technologies with these features and characteristic will enhance the organizational effectiveness and Alliance operations by development of the knowledge and decision advantage. In addition, it has been found that the implementation of this technologies in the upcoming future will enhance effectiveness of the mesh capabilities throughout all the instruments of power and operational domains (Reding & Eaton, 2020).

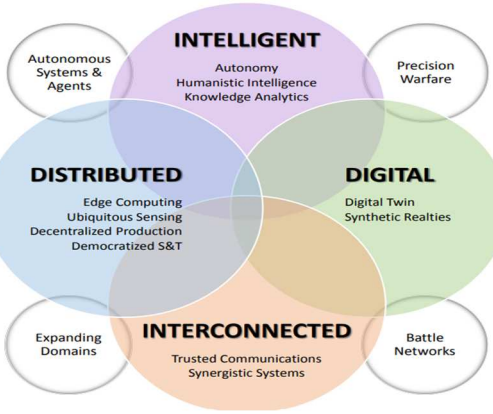


Figure 5: Science and Technology Trends

Moreover, studies show that there are eight highly interrelated science and technology areas that are considered as the significant strategic disruptor for the next 20 years. The defence minister approved the first seven EDTs in October 2019; however, an eighth EDT is added for future development and consideration by STO. These Science and Technology areas are either undergoing rapid revolutionary development or are in the nascent stages of development. These EDT's include Artificial Intelligence, Data, Quantum, Hypersonic, Space, Autonomy, Biotechnology and Materials. Additionally, the new emerging technologies in the military organizations are defined under three major categories; Emerging, Convergent and Disruptive. Emerging technologies are those scientific discoveries and technologies that are considered to reach the period of maturity by the year 2020-2040 (James, 2013). However currently these technologies are not widely in use and are not the ones whose impact on security, Alliance defence, and enterprise function are not clear entirely. The convergent technologies are defined as the ones that have combination of various technologies and these combinations are made in novel manner for creating disruptive impact. Lastly, the disruptive technologies are defined as those scientific discoveries and technologies, that will have significant and revolutionary impact on the NATO defence, enterprise or security functions during the period of 2020-2040. The intelligent technology will include knowledge analytics, humanistic intelligence and autonomy; The distributed technology will include the Ubiquitous sensing and edge computing, democratised science and technology, and decentralised production; The interconnected technology will include the trusted communication, and synergistic system; Lastly the digital technology will include the synthetic realities and digital twin (Reding & Eaton, 2020).

III. THE DIFFERENT STRATEGIES AND FRAMEWORKS THROUGH WHICH LATEST IT TECHNOLOGIES COULD BE USED IN MILITARY ORGANIZATIONS:

The implementation of IT technologies in Military organizations and a well-structured digital transformation plan is a significant business strategy. Thus, for implementing digital transformation plan successfully the military

organizations should start with proper road map that is guided by business outcomes and then they should pair their strategic plans and initiatives with the technology-related initiatives. The following strategic plan could be used by the military organization to implement the use of IT technologies:

A. *Establishing the goals and objectives of the organization:*

In every organization the implementation of digital transformation may look different because of available factors like the familiarity of the employees with technology, budget and the available resources. Thus, the goals and objectives may vary according to this. However, establishing business goals, needs and objectives at first helps in building an effective strategy and is first step toward implementing digital transformation. While establishing the goals and objective the military organizations should establish their new revenue models, adapt to change in the market dynamics, and accelerate the existing revenue models. This will help the organization to bridge the gaps and establish the foundation of digital transformation by defining business priorities and values.

B. *Focusing on the change in organizational culture:*

In the implementation of digital transformation cultural change comes automatically and it disrupts the workforce engagement and facilitates the rise of the new digital culture. Therefore, it is crucial for military organization to focus on cultural change and make sure that their workforce adopts to the change is culture smoothly. Hence for dealing smoothly with the cultural change and adopting the digital transformation the military organization should ensure that they explain the what, how and why process, establish a culture of innovation and collaboration, articulate the potential business outcomes and benefits and develops a team mindset among the workforce (Jupudi, 2022).

Figure 6: Digital transformation in military organization

C. *Implementing the Information Technology wisely:*

In the implementation of digital transformation in military organization choosing the technology is a crucial step. The technology that should be implemented in digital transformation should fulfil the needs of the company and should align with the objectives and goals that was established earlier. Some of the efficient technologies that will help in successful digital transformation are the internet of things, cloud computing, machine learning, artificial intelligence, virtual reality or augmented reality and robotics. Further the new technologies should be implemented with improved operation, because if the internal process in not updated there is no point of implementation of new technologies.

D. *Creating partnership with experts:*

It is recommended to have partnership with firms that are expert in digital transformation, because implementing IT and digital transformation is a complicated task and if the organization is doing such organizational change for first time, then collaborating with expert firm is beneficial. The military organizations should also establish a particular research and development centre for strengthening their cyber security skills and should also strengthen their data and information by implementing blockchain and big data analytics.

E. *Leaving the room for agility:*

Agility and effective planning is important for successful digital transformation in any organization, as this provides long-term sustainability and it also reduces the chances of failure. Therefore tracking, analysing and observing post-implementation will help the military organization to identify the loopholes that block the progress, understand which strategy is working and which is not working and change the plan accordingly on the basis of feedbacks from the system and users.

IV. DATA METHODOLOGY

A. *Research approach:*

In order to develop the research, report the deductive research method has been used. The adoption of the deductive research approach has helped in investing the research topic effectively, with aid of deductive approach the current and future trends of Information Technology in the Military organization has been investigated properly. This has helped in gathering relevant data about the research topic and also provided with better understanding about digital transformation in military organizations.

B. *Research design:*

The research paper has been developed by following the exploratory research design. This research design is chosen because it is considered to appropriate for developing reports on qualitative data and information. The research report is qualitative in nature and the information are collected from different articles and journals of various authors.

C. *Data collection method:*

In order to gather data and information of the research report the secondary method of data collection has been used. The researcher has gathered relevant and authentic data by analysis and researching different journals and articles thoroughly. The data and information collected for the study is non-numeric and is totally based on theoretical data.

D. *Data analysis method:*

The research report analysis the collected information and data using the thematic analysis method. The information gathered from the articles and journals are presented in the literature review section theme wise, and the analysis is done

as per that. Further the findings and discussion section in the report sheds light on the major findings of the study.

V. Findings and Discussion

The findings of the study highlights that most of the military organization are showing their interest in implementation and development of new technologies like Artificial Intelligence, Machine learning and autonomous technologies. The organizations are investing heavily on their research and development centre for developing these technologies and transforming their traditional military organizations into smart military organizations. It has also been found that now a days the military organizations are finding themselves in dynamic, complex and data-driven environments, and therefore to respond to these changes and to become adaptable and flexible to the new environment the military forces are investing huge amounts in Information Technology. The Military organization believes that implementing the new technologies will help them to become flexible and adapt to the changes quickly.

It has also been found that the rapid changes in these technologies are also increasing the malicious cyberthreats and are putting the military organizations at risk. The government and defence organizations have sensitive data and information that could leads to war or put any country with security risk, therefore it has become crucial for military organization to adopt proper strategies to strengthen their cyber security. The findings highlight that the U.S is having increased their budget of cybersecurity and they have understood the importance of developing a strong cyber security centre at their military organization. Further the findings show that the U.S, China and Russia are paying much attention in implementing the new and advanced technologies in their military organization, among this three countries U.S is the leading one in innovating and implementing Information Technology in DoD, China comes next to U.S and Russia is trying its best to maintain pace with these two countries. It has been found that U.S, China and Russia have already implemented the use of Artificial Intelligence in their military organizations and they are trying to develop it more. Additionally, it has been found that the countries are also focusing on implementing Quantum technology in their Military organization and in the year 2017 China established the -first quantum-secured intercontinental video conference.

VI. Conclusion

The information technology will drive the future battles, the military forces will continue their battle on sea, land, in space and in sky, but those who will have superiority on situational awareness and will be empowered by innovation in Artificial Intelligence, Virtual reality, edge computing and big data analytics will win the battles. The completion of the research report provides detailed knowledge about the importance of Information Technology and Digital Transformation of Military Organization in the modern world. The study sheds light on the need and requirements of the military organization to keep pace with the changing environment. The study shows that it has become crucial for nations and alliance to understand the readiness, potential impact and synergies that are associated with EDT. The Emerging Digital Technologies are expected to provide a significant impact both positive and negative on the military organizations over the coming 20 years (Reding & Eaton, 2020). However, implementing these new technologies in the organization will raise many challenges, but facing these challenges effectively will help organization to successfully implement the digital transformation. The research report discusses about the potential strategies that could use by the military organization to implement digital transformation. The expansion of the use of autonomy, BDAA and AI will provide the organizations with greater accessibility to critically operate relevant information and data. The study also highlights that, in today's time cybersecurity has become essential for accomplishing objectives and mission of an organization, thus the organization should not only rely on adopting new technologies rather they should also institute a culture of cybersecurity in their organization. If there is no shift in the culture of the organization then they might face challenge in adopting these technologies from budget perspective and employee perspective. Hence, the organization should focus on developing a change process that is smooth and easy to accept for the employees (Golden, 2016).

References

[1] A. D. James, "Emerging technologies and military capability - ETH Z," 2013. [Online]. Available: https://www.files.ethz.ch/isn/174574/Policy%20Brief-Emerging%20Technologies%20and%20Military%20Capability.pdf. [Accessed: 10-Dec-2022].

[2] "Chief information officer - U.S. department of defense," Chief Information Officer - U.S. Department of Defense. [Online]. Available: https://dodcio.defense.gov/. [Accessed: 10-Dec-2022].

[3] D. Golden, "How military strategy can improve cyber response," FCW, 26-Jan-2022. [Online]. Available: https://fcw.com/security/2016/07/how-military-strategy-can-improve-cyber-response/220317/. [Accessed: 10-Dec-2022].

[4] D. Snyder, J. D. Powers, E. Bodine-Baron, B. Foz, L. Kendrick, and M. H. Powell, "Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles," 2015. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA623202.pdf. [Accessed: 10-Dec-2022].

[5] "Defense Technical Information Center," Page Redirection. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1131124.pdf. [Accessed: 10-Dec-2022].

[6] "Dni.gov," 2021. [Online]. Available: https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf. [Accessed: 10-Dec-2022].

[7] J. Fidock, "Organisational Structure and Information Technology (IT): Exploring the Implications of IT for Future Military Structures," DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) COMMAND AND CONTROL DIV., 2006. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA458912.pdf. [Accessed: 10-Dec-2022].

[8] J. Ryseff, "How the military might expand its cyber skills," RAND Corporation, 22-Apr-2021. [Online]. Available: https://www.rand.org/blog/2021/04/how-the-military-might-expand-its-cyber-skills.html. [Accessed: 10-Dec-2022].

[9] K. M. Sayler, "Federation of American scientists," 2022. [Online]. Available: https://sgp.fas.org/crs/natsec/R46458.pdf. [Accessed: 10-Dec-2022].

[10] P. F. Nunes, "The impact of new technologies in the Military Arena ... - air university," 1999. [Online]. Available: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/nunes.pdf. [Accessed: 10-Dec-2022].

[11] S. Jupudy, "How to implement a digital transformation plan in five steps," Bizjournals.com, 2022. [Online]. Available: https://www.bizjournals.com/dallas/news/2022/03/24/how-to-implement-a-digital-transformation-plan-in-five-steps.html. [Accessed: 10-Dec-2022].

[12] T. Nurtin and M. Konaev, “Eye to eye in AI: Developing artificial intelligence for national security and defense,” Atlantic Council, 07-Jun-2022. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/eye-to-eye-in-ai/. [Accessed: 10-Dec-2022].

[13] “U.S. Army Strategic Cyber Posture - events.afcea.org.” [Online]. Available: https://events.afcea.org/afceacyber22/Custom/Handout/Speaker149820_Session9403_1.pdf. [Accessed: 10-Dec-2022].