THE EFFECT OF TECHNOLOGICAL TRANSFORMATION ON THE MANAGEMENT OF SECURITY STRATEGIES

Mehmet Naci EFE[1]

Abstract

This article examines the effects of new technologies that emerged in the 21st century on security and thus on the battlefield. The battlefield, the actors in war and conflict, and the threat perception have changed drastically with both the technology and the socio-political effects of globalization. In such an environment, the countries that want to be strong in the international political, economic and political arena and aim to protect their national interests, always want to be ready for all kinds of threats besides conventional wars and threats and to develop technology in order to gain a share in defense industry with a large market and to import military applications. The military, which is the guarantee of the security of the countries, uses the new technology in order to minimize the damage to himself and to give maximum damage to the enemy.

Keywords: Technology, Security, Soldier, Security Strategies, Technologic Transformation.

TEKNOLOJİK DÖNÜŞÜMÜN GÜVENLİK STRATEJİLERİNİN YÖNETİMİNE ETKİSİ

Öz

Bu makale 21. yüzyılda ortaya çıkan yeni teknolojilerin güvenlik ve dolayısıyla muharebe sahasındaki etkilerini incelemektedir. Muharebe sahası, savaş ve çatışmalardaki aktörler ve tehdit algısı hem teknoloji hem de küreselleşmenin getirdiği sosyo-politik etkilerle büyük ölçüde değişime uğramıştır. Böyle bir ortamda uluslararası politik, ekonomik ve siyasi arenada güçlü olmak isteyen ve milli çıkarlarını korumayı amaçlayan ülkeler konvansiyonel savaşların ve tehditlerin yanında her türlü tehdide karşı her zaman hazır olmak istemekte ve büyük bir pazara sahip savunma sanayiinde pay elde edebilmek için teknolojinin geliştirilmesi ve askeri uygulamalara ithal edilmesi için yoğun gayret sarf etmektedirler. Ülkelerin güvenliğinin teminatı olan askerler yeni teknolojiden savaş ortamında hem en az derecede zarar görmek hem de düşmana azami hasarı vermek için yeni teknolojiyi kullanmaktadır.

Anahtar Kelimeler: Teknoloji, Güvenlik, Güvenlik Stratejileri, Teknolojik Dönüşüm.

[1] Doç. Dr., efemehmetnaci025@gmail.com, ORCID: 0000-0001-7039-5659

Introduction

As a result of the rapid progress of technology, new methods, and techniques are emerging in process technology and manufacturing technology. Existing technologies are rapidly losing their usefulness as a result of technological progress and are being replaced by more sophisticated, better technologies. Corporate and business-based technology management is very important in order to keep up with the rapidly developing technology. Technological developments constitute an important area of interest within the scope of security in the Armed Forces, which is the first responsible institution for the defense of the country, like all institutions. Ensuring that the security forces keep up with technological developments is important in terms of combating dangerous formations. Therefore, security forces develop strategies to catch up with technological developments and facilitate management.

Technological advances provide security forces with advanced tools and systems to collect, analyze and disseminate information. This leads to improved situational awareness, enabling security administrators to make more informed decisions and develop more effective strategies to address emerging threats. Advanced technologies such as artificial intelligence, big data analytics, and unmanned aerial vehicles (UAVs) have revolutionized intelligence and surveillance capabilities. Security administrators can leverage these technologies to gather real-time intelligence, monitor activity, and detect potential threats more efficiently. This enables proactive decision-making and allocating resources where they are needed most. Rapid advancement in technology brings with it new cybersecurity risks and challenges. Security managers need to adapt their strategies to counter cyber threats and protect critical infrastructure and sensitive information. They need to stay up to date on the latest cybersecurity measures and invest in robust defense mechanisms to mitigate potential vulnerabilities. Technology-driven security strategies require the integration and interoperability of various systems and platforms. This includes seamless communication and data sharing between different security agencies and stakeholders. Security administrators need to ensure that different technological components work together effectively to achieve a comprehensive and coordinated approach to security. Technological transformation necessitates continuous training and skill development for security personnel. Security managers should invest in training programs to equip their teams with the necessary expertise to operate and manage advanced technologies. This ensures that security strategies are effectively implemented and optimized. The adoption of emerging technologies in security strategies raises ethical and legal considerations. Security managers must address complex issues such as privacy, data protection, and adherence to international norms and regulations. Establishing guidelines and frameworks to ensure the responsible and lawful use of technology in security management is crucial.

The aim of this study is to reveal the direct effects of the developments in technology on the

scope of security in military technologies.

Literature Review

Concept of Security

Security refers to the state of being protected against dangers, threats, risks, or harmful effects. In general, it includes measures taken to protect individuals, communities, organizations, or systems against various hazards and to minimize these hazards. Security can mean different things in different contexts. For example, physical security means protecting people and assets from physical danger. Such security measures may include the protection of buildings, facilities, borders, vehicles, and other physical assets. Examples may include security cameras, barriers, alarm systems, and security personnel. Information security refers to the protection of electronic data and information against unauthorized access, manipulation, or harmful effects. Such security measures may include data encryption, security software, access controls, and network security solutions. Cybersecurity includes protecting against threats and attacks on computer systems, networks, and digital devices. Measures taken against threats such as viruses, malware, and cyber-attacks are a part of cyber security. Personal security aims to ensure that individuals feel physically safe and protected from dangers. This may include being in safe zones, avoiding hazardous situations, and using personal safety equipment. In the context of international relations, it refers to the measures taken against international security, war, terrorism, armament, and other global threats. International security is handled through international organizations and treaties. The concept of security includes a set of strategies, policies, and technologies that are planned, implemented, and maintained based on risk analysis and threat assessments. Security aims to ensure the stability and sustainability of individuals, communities, and systems. The concept of security is related to the efforts of states, societies, groups, and individuals to protect and maintain their survival (Dedeoğlu, 2004). This includes adopting various measures, tools, and policies to counter any potential threat. The concept of security may change in response to prevailing situations and conditions.

The idea of security is commonly discussed in the field of international relations, but its definition can be unclear. Buzan (1991) noted that security is a complex and often contested concept, closely related to power, freedom, and love. This has led to ongoing theoretical debates and disagreements about its meaning. McSweeney (1999) argued that security is multifaceted and can be connected to various other concepts, such as peace, dignity, and justice, but a definitive definition is difficult to establish. Baldwin (1997), on the other hand, described security as a controversial term that is easily confused and poorly explained. Baldwin suggested that two key questions can help define security: "Who is security sought for?" and "What values are protected by security measures?" Baylis & Smith (2008) generally characterize security as being free from threats to core values. Some scholars differentiate

between objective and subjective security and argue that the concept is meaningless without a perceived threat (Lipschutz, 1995). According to Wolfers, security refers to being free from potential harm to an objectively owned value, while at the subjective level, there is no concern that the value in question will be attacked (Baysal & Lüleci, 2015). It is also important to consider how the concept of security has been affected by history, such as during the Cold War, and its current relevance.

Security Strategies

The strength and resilience of citizens, communities, and the economy are crucial for national security, according to the White House in 2010. Security strategies aim to establish objectives that protect the country's life and property, increase the strength and resilience of citizens, communities, and the economy, identify potential threats and opportunities, and achieve these goals. It acknowledges the critical role of power in international politics and defines national interests, as outlined by the White House in 2018. Security is a complex problem that encompasses both logical and physical issues, as noted by Sveen in 2009. Long-term planning or strategic planning serves as the foundation for designing security strategies, according to Snider in 1995. A strategy is a policy-making tool that outlines long-term objectives to be achieved and the main categories of instruments to be applied, providing a frame of reference for day-to-day policy-making in a rapidly changing and increasingly complex international environment, and guiding the identification of both civilian and military capabilities (Biscop 2005: 1). Security strategies are designed to address a variety of complex issues such as terrorism, drug trafficking, organized crime, environmental damage, resource depletion, rapid population growth, new infectious diseases, and uncontrolled refugee migration (White House, 1998). Consistent use of tools such as political, diplomatic, development, humanitarian, crisis response, economic and trade cooperation, and civil and military crisis management are necessary for prevention of these threats (European Council, 2003). In order to shape a security strategy for modern times, it is crucial to understand the current trends, what has changed, what remains unchanged, and to appreciate the opportunities and dangers that history has presented to us (White House, 1991). Climate change has also been included in security strategies due to its significant impact. The limited availability of energy sources like oil is now regarded as a threat to security strategies, which has led to an increased focus on evaluating diverse energy sources and renewable energy in security strategies. With the rise of digital and technological transformations in organizations and businesses, the storage and evaluation of information and data in the digital realm, and the increasing use of robots and artificial intelligence, cyber security has become a crucial component of security strategies.

Organizations and countries adopt security strategies to ensure their safety, protect against threats, and manage risks. These strategies start with an evaluation process to analyze current

and potential threats, including internal and external threats, trends, strategic weaknesses, and risks. This threat assessment forms the basis of security strategies and enables the appropriate measures to be taken against risks. Security strategies take a comprehensive approach that includes not only military force but also political, economic, diplomatic, and social means. To achieve this, various policy areas and stakeholders must be brought together and coordinated. Security strategies address security areas that affect society as a whole. Priorities are set in line with identified threats and risks, such as dealing with urgent threats, protecting critical infrastructures, and fighting terrorism. Long-term goals and sustainable security policies are also included. International cooperation and partnership are crucial to carrying out security strategies. Information sharing between countries and institutions, military and intelligence cooperation, technical assistance, and joint work on other security issues are all part of the strategy. Collaboration and partnership are vital in providing a more effective defense against common threats (Pronoza et al., 2022). Effective security strategies are crucial for protecting organizations and systems from constantly evolving threats. To achieve this, security policies must be regularly reviewed and updated to incorporate new technologies and strategies that adapt to the changing security environment. Security strategy management involves developing, implementing, monitoring, and continuously improving strategies aimed at ensuring the security of an organization or system. These strategies may cover areas such as information technology security, physical security, and business continuity management.

To begin developing a security strategy, it's essential to identify potential risks and threats to the organization. This involves identifying valuable assets, analyzing potential threats, and identifying any vulnerabilities. Based on the risk assessment, the organization can determine its security goals and develop strategies to achieve them. These strategies may include preventive measures, detection mechanisms, response plans, and communication protocols. Once developed, the strategies are implemented through the installation of security solutions, personnel training, and the implementation of processes.

Continuous monitoring and auditing mechanisms are put in place to assess the effectiveness of security measures. In the event of a security incident or crisis, predetermined crisis management plans will come into play, which may include rapid response, communication strategies, and business continuity solutions. After the events, the effectiveness of the interventions and measures taken are evaluated, and improvements are made to the strategies if necessary.

It's essential to note that security strategies are an ongoing process that must be reviewed and updated regularly. With technological advancements, new threats, and organizational changes, security strategies need to adapt to the changing needs of the organization and

innovations in the security landscape. By continuously reviewing and improving security strategies, organizations can ensure that they are always prepared to face potential security threats.

Cold War Era Security Approaches

The concept of security in international relations is influenced by various factors such as the system's structure, historical conditions, international context, actors involved, and their relationships. The field of international relations observes practice-theory dependence and interaction through different theoretical approaches. During the 1945-1990 period, security studies showed stagnation and uniformity similar to the static bipolar structure of the Cold War era. Security is a fundamental concept in international relations, and realism and neo-realism were the dominant paradigms during the Cold War. In the late 1960s and early 1970s, liberal thought and neo-Marxist approaches questioned the classical understanding of security, leading to a transitional period in security studies. However, realist and neo-realist security paradigms dominated the two-block structure and were determined by basic assumptions of thought. The traditional security paradigm is state-centered, national security indexed, power-oriented, especially military power, and its ontological framework reflects the main arguments of realist theses. The Cold War security paradigm has been replaced in the literature by the traditional security understanding, which is dominated by classical realism and neo-realism, and portrays the identity and practice of the bipolar system as hegemonic and status quo (Sandıklı & Emekliler, 2014).

A New Understanding of Security After the Cold War

The balance between "us" and "other" entities within a system can facilitate the creation of alliances and definitions of threats. This was observed during the Cold War era, where actors sharing similar ideologies assumed roles in different factions while maintaining their relationships amid existing divisions. In the post-Cold War era, as systems become more complex, actors' confidence in their ability to manage and adapt to differences increases. In the contemporary global system, security and threat definitions are diverse, with similarities and differences coexisting and expanding. The proliferation, expansion, and complexity of security present significant challenges to traditional security discourse, leading to the emergence of alternative security studies. These studies aim to address questions about actors, objectives, locations, and methods of security. Post-positivist theories, including critical, post-modern, feminist, and constructivist perspectives, question the traditional security paradigm. However, the Copenhagen School, which actively studies security and proposes important arguments, is working towards creating a new understanding of security(Sandıklı & Emekliler, 2014).

The Copenhagen School, which includes notable figures like Buzan, Waever, and security

experts such as Jaap de Wilde, Morten Kelstrup, Pierre Lemaître, and Elzbieta Tromer, is situated at the Center for Peace and Conflict Studies in Copenhagen. McSweeney originally provided the terminology for this academic institution, which was later widely adopted by the academic community and group members. According to Huysmans, the institution has dual objectives: to safeguard security from the limiting effect of military-political perspectives and ensure conceptual integrity (Huysmans, 2007). The Copenhagen School has made significant contributions to the academic literature on international security studies by developing three major theories: securitization/de-securitization theory, sectoral security approach, and regional security complex theory (Baysal & Lüleci, 2015).

The concept of security is constantly evolving with technological advancements. For instance, virtual reality simulations allow military personnel to gain valuable experiences, improve their abilities, and develop their training budgets without difficulty, thus offering security benefits and cost savings (STM, 2018a). The new war environment involves land, sea, air, space, and cyber warfare dimensions (Akçay, 2018). The new generation war environment is a war environment in which countries use their political, economic and political power as a tool, along with the use of conventional weapons. In this warfare environment, technology is used intensively (Erdoğan et al., 2022). Countries are now engaging in network and space operations instead of relying solely on military power to defeat their opponents. The increasing significance of satellites in military operations has led to the proliferation of space warfare. Countries aim to immobilize their adversary states by blinding their satellites (STM, 2018b)

Technological Transformation

The use of steam-powered machines in factories at the end of the 18th century, the start of mass production based on electrical energy in the early 20th century, and the widespread use of automation in the industry by means of electronics and information technologies since the 1970s, provided a great increase in industrial efficiency with the advancing technology (Öztürk, 2017). The industrial efficiency brought by the development of technology has increased the importance that organizations attach to the necessity of innovation. Efficient use of knowledge requires a transformation process that includes designing applications for new scientific concepts and transforming these applications into viable technologies, products, or services (Fontes, 2005). Innovations do not occur randomly, they are created on the basis of existing capabilities in organizations and social systems, and their further development depends on the need for a new product and the existence of a system in which it can be produced and used (Ende and Kemp, 1999). The technological environment is based on the characteristics of knowledge, the accumulation of technical progress (today's knowledge and innovation activities are the basis and building blocks of tomorrow's innovation), the relevance of innovation (the opportunities to protect innovations from

imitation and profit from innovative activities), technological opportunities (the possibility of innovation corresponding to R&D investments).) depends (Breschi, 2000). Innovation processes are complex because they typically depend on the co-development of new socio-technical configurations, new market structures, new actors, and new institutional environments (Markard, 2008). Technological transformation processes can be triggered by new guiding principles, design criteria, or other requirements, or can be initiated by the development of new works, new technical tools, or design tools (van de Poel, 2003). Technological transformation can increase the interdependence of products and technologies. The commitment to products, devices, and people increases the efficiency of production machines and equipment, reduces costs, and saves resources (Kohnova, 2019). Computer, information, communication, and multimedia technologies have changed and are changing everything from the way people work to the way they communicate with each other and spend their free time (Kellner, 2004).

Technological transformation has affected and continues to affect security in terms of making products more suitable for use, reducing their visibility, reducing their volume, expanding their scope, and protecting critical data. In particular, studies on the formation of technological activities and innovations for the asymmetric war environment have increased. Preventing loss of life and property is realized by conducting effective technological studies. Artificial intelligence, robots, and UAVs can prevent the loss of soldiers and property by taking part in activities that can be considered risky.

The Concept of Technology and Developments in Recent Years

Technology, which develops and changes at an extraordinary rate in our age, fundamentally affects and changes the cultural structure and armies. This change also includes the content of the image in question: the concept of "technology" develops, diversifies, and acquires many different features. The interesting aspect of the subject is that there is a parallelism between what a nation acquires from technology, in other words, how this image fills itself and its place in technological development. (Ural, 2016). The root of the word technology, which means the application knowledge that covers the construction methods related to an industry, the tools, equipment, and tools used, and the way they are used, is 'Technologia'. It is formed from the combination of the words “techne” meaning “mastery, ability to do” and “logy” meaning “to tell” in Ancient Greek (Türk Dil Kurumu, 1988). Except for the meaning in the dictionary, the concept of technology has different definitions and different perspectives according to occupational groups. For example, according to engineers, it is the sum of the logistics methods used during the production of a product, but according to the occupational groups interested in the economy, it is seen as a tool that increases the welfare levels of countries and therefore nations (Altın, 2014).

Many people associate technology with physical hardware, but it also has a virtual (software) aspect. The physical dimension involves the materials utilized, while the software dimension involves the education and training methods or management styles specific to the business group that employs the technology (İşman, 2014). Technology has been defined in various ways. For example, Demirel (1993) defines technology as the application of observational and proven knowledge to achieve goals and solve problems. Alkan (1998) defines technology as the creation of functional units that enable the domination of nature by activating acquired capabilities. Technological advances have brought about improvements in weapon systems, just as they have in other fields. New technological systems have been incorporated into new weapons or entirely new weapons have been produced. This development of technology has altered defense planning and introduced new concepts. As a result, countries must consider space, cyber threats, and nuclear and asymmetric war environments when developing their defense plans in today's circumstances. To illustrate the impact of technological advancements on defense planning, it is essential to discuss some recently produced systems that have been employed in the field of defense.

UAVs

An unmanned Aerial Vehicle (UAV) is a type of unmanned aerial vehicle that can fly autonomously or remotely, has its own power source, and can carry both lethal and non-lethal elements. UAVs do not include ballistic and semi-ballistic missiles, cruise missiles, or artillery-fired munitions. The United States is known for developing the technology behind UAVs, also known as "drones", "robot airplanes", "non-pilot airplanes" and "remotely piloted airplanes". UAV Systems are systems created by adding ground control stations, ground data terminals, and other equipment to provide flight and mission capability to UAVs (Akyürek, 2012). UAVs are aircraft that can fly without human intervention and are usually guided by remote control or automatic controls. UAVs are used for various purposes. UAVs play an important role in defense and security strategies along with technological developments. The military capabilities currently available in UAVs or anticipated to be acquired in the near future can be listed as follows:

- Reconnaissance, tactical reconnaissance, and surveillance
- Bomb or missile air strikes
- Forward surveillance for indirect (invisible) shots
- Special operations and psychological operations
- Control and protection of borders
- Mine search and destruction
- Replenishment of health and military equipment
- Fight against smuggling
- Chemical, biological, and radiological scanning

- Ship identification and isolation in maritime
- Combat search and rescue
- Extending flight time with aerial refueling
- Air radio link and relay duty
- Point-to-point cargo delivery
- Weather data collection

Stealth Planes

Stealth planes, as the name suggests, help pilots evade detections in the sky. While aircraft are completely invisible for radar detection, stealth aircraft use a variety of advanced technologies to reduce aircraft reflection, the radio frequency spectrum, and radar and infrared emissions. Stealth technology increases the probability of a successful attack because enemies have difficulty finding, tracking, and defending these aircraft (Chow, 2013). Stealth aircraft are specially designed aircraft that are less visible to radar detection systems and minimize the radar trace. Stealth technology relies on aircraft absorbing radar waves rather than reflecting them, or minimizing their reflection. This reduces the risk of early detection by enemy radars and enables the aircraft to perform attack or reconnaissance missions more effectively. In stealth aircraft designs, low radar cross section (RCS - Radar Cross Section) is generally targeted. For this, factors such as the shape of the aircraft, the use of materials, surface coatings, and exhaust gases are optimized. For example, aircraft surfaces are designed in flat and irregular shapes, corners are rounded, and materials that absorb or reflect radar waves are used. In addition, it is important that the engine exhausts also have special designs to minimize heat and radar signature. Stealth aircraft are often used for special operations such as reconnaissance, air superiority, and strategic attack missions. These aircraft are technologically advanced platforms that enable effectiveness in covert operations, represented by examples such as the F-117 Nighthawk, B-2 Spirit, and F-22 Raptor. Stealth technology is constantly being developed and used as part of aircraft designs to provide an advantage over modern air defense systems. There are many such systems that can be counted. The main point to draw attention to is how these systems contribute to the understanding of security. We can assume that countries use the following justifications when integrating technology into their defense systems.

- Reducing collateral damage
- To prevent civilian casualties
- Using more effective weapons
- Fewer soldiers on the battlefield (Lister, 2017)

Future Technologies

In the unmanned armies of the future, troops, especially humans, will be replaced by robots that choose their strategies and tactics and fulfill their duties endlessly, whether they need a limited operator or not. The military is where technology is used the most. This is because the demands are constantly changing and increasing. Even so, most of the technology used in the weapons of the future is quite advanced. These include autonomous driving, artificial intelligence, and machine learning. Unmanned armies of the future will have robots that can be used for attack, defense, and even rescue (Habertürk, 2017). Advances in artificial intelligence and machine learning continue unabated. Improvements are expected in areas such as smarter and autonomous systems, better natural language processing capabilities, and more effective image and sound analysis. IoT devices and applications will be adopted in different areas of life, from homes to industrial facilities. Thanks to the Internet of Things, communication between devices will increase and data collection, analysis, and management will become more efficient. 5G technology will reach a wider coverage area, offering faster internet speeds, lower latency, and more reliable connections. This can support the development of technologies such as virtual reality and augmented reality. AR and VR technologies will be used more in different sectors such as entertainment, education, healthcare, and business. Further investment in these technologies is expected to deliver more realistic experiences and interactions. Autonomous vehicles and driverless transport systems can lead to significant developments in the automotive industry. The security of these systems, legal regulations, and infrastructure issues continue to be important discussion points. Environmentally friendly and sustainable technologies will gain more importance in areas such as energy production, waste management, and water saving. Studies on the development of renewable energy sources and energy storage solutions will continue. Technological advances in medicine will continue, and there may be advances in areas such as personalized treatment methods and gene editing technologies. Quantum computers have the potential to perform complex calculations much faster. Research and developments in this area will continue to be important. Advances in gene editing, biotechnology, and biomaterials can have implications for health, food production, and the environment. Space technologies can continue to advance towards big goals such as Mars exploration. In addition, space tourism may also become open to more people.

The reasoning and conclusions that are possible through algorithms will be realized. Artificial intelligence stands out with the potential it offers in the fields of rapid decision-making, regeneration and high performance, training, and intelligence/reconnaissance skills that a strong army should have. Artificial intelligence can make decisions much faster than humans, based on inputs in today's multi-axis work environment. A damaged limb can be reconstructed, and autonomous systems are easy to build in their entirety. Also, they never get tired. Artificial intelligence weapons have much greater accuracy than human weapons, as they can calculate a large number of possibilities as a result of powerful processing.

Artificial intelligence applications in areas such as personnel training, fighter pilot training, and technical training, when used with augmented reality, can provide an advantage for the Armed Forces within the existing force structure. It will facilitate the rapid and accurate analysis of data in large areas. Searching enemy elements will be easily detected thanks to face recognition technology. (Kendi, 2018).

Another issue related to artificial intelligence (Internet of Things - IoT) is the Internet of Things. To put it simply, the Internet of Things is a concept that means that all devices with on/off buttons are connected to the internet and/or each other (yeniisfikirleri.net, 2018). The rapid emergence of the Internet of Things has spawned two technological arguments: machine intelligence and networking. When people use their intelligence correctly, they can do more effective and productive work. This may equally apply to new uses that are planned to have artificial intelligence that is predicted to take place in future wars. Robots, too, can better serve human warriors when they manage to have intelligence and coordinate their actions among themselves. This is called the Internet of Battle Things (IoBT). In some ways, IoBT is already becoming a reality, but it is expected to be heavily involved in wars 20-30 years from now (Kott, Swami, & West, 2016). It is considered that the battlefield of the future is likely to be densely populated with such objects. In light of all these reasons, these systems, which aim to cause the least harm to their own people and the maximum harm to their opponents, will of course find a place in the new security concept.

Management

Management is the process of effectively planning, organizing, coordinating, directing, and controlling resources (human, material, time, finance, etc.). It is the process of using resources in the most effective and efficient way to achieve the goals and objectives of an organization or group. Although the concept of management is often associated with businesses and organizations, it actually takes place in many different contexts in daily life. It is the phase of setting goals, allocating resources, formulating strategies, and preparing action plans. Planning determines where the organization wants to go and how it will get there. It includes organizing resources and tasks in the best way possible. At the organizational stage, issues such as who will do what and who will take on which responsibilities are determined. It is the stage of establishing collaboration and harmony between different departments, teams, and functions. Coordination involves arranging how different parts work together. It includes motivating people, guiding, leadership, and communication. The guidance supports employees in achieving set goals. It is the phase of monitoring the realized activities, measuring the results, and evaluating how close the targets are. Control evaluates compliance with the plan and achievement of goals. Management includes a wide variety of elements such as leadership, organizational structure, decision-making, and communication. Good management aims to achieve the determined goals by using the resources in the best way.

While management ensures the sustainability and effectiveness of businesses, it can also be applied in various fields such as groups, projects, and personal life.

The main tasks of management, whether it is a commercial enterprise, hospital or university, are to realize the specific purpose and mission of the institution, to make the work productive and to enable the worker to complete the work, and to manage social impacts and social responsibilities (Drucker, 1974). It is to create value by helping people become more productive and innovative through a collaborative effort (Magnetta, 2003). Business plans ask management to logically analyze the business in a structured way and think about what it is doing now and what it wants to do in the future (Burtonshaw, 2008). The selection of objectives, the selection of products to be delivered by all services, the design of the entire organizational structure, the administrative systems, all the policies used to define all coordinated work (Rumelt, 1991) constitute the scope of its management. Management proposes to focus on managing control and currently existing resources (Skyrme, 2000). Management understands that maintaining a loyal customer base requires continuous improvement of products and services (Oz, 2009). Management should provide leadership, motivation and supervision, especially if it requires significant changes in business processes, organizational structures or roles and responsibilities (Kumar, 2006: 41). An ideal management system is one in which power is automatically redistributed when environmental changes devalue managerial knowledge and competence (Hamel & Breen, 2007). In the world where technology and the virtual world have begun to dominate, concepts such as knowledge management and management innovation have been valued. Technological transformation brings the security of robots, artificial intelligence, smart cities and smart systems to the agenda in security management. Governments and private sectors have accelerated their work for cyber security. These studies led to the creation of cryptographic keys and anti-virus programs.

Conclusion

Managing security risks is crucial for organizations to respond effectively to crises and improve their security measures. The approach to security strategy may vary based on factors like the organization's type, size, and industry. The concept of war has evolved with time, affected by political, socio-cultural, and economic factors like country politics, power dynamics, and international relations. The events of the twenty-first century have demonstrated that change is a constant factor in our understanding of international security (Astan, 2015).

As technology continues to advance, it brings about new opportunities in various fields. Sometimes, these developments work in tandem, while at other times, they operate independently. Upon examining the evolution of technology from ancient times to the present day, it becomes clear that every era has either created or benefited from fundamental tools.

Like every other industry, the military also relies on technological progress to enhance its security measures (Meydan, 2015). Technological breakthroughs give nations a competitive edge in preparing for security and defense, making high-cost and long-term supply projects a worthwhile investment. These advancements have led to significant changes in the security perception of countries, resulting in new doctrines, concepts, and organizational structures. Additionally, new battlefield dimensions, such as space, cyber, and network-centered operations, have emerged. The development of unmanned vehicles and aerial drones has become increasingly critical in recent years, as they can be used as both combat support and combatants, with the aim of minimizing harm to human life. All these advancements are geared towards ensuring the welfare and survival of people, as well as giving countries a voice on the world stage. As technology continues to evolve, it is expected that these developments will become even more prevalent in the future.

To sum up, the advancement of technology has a significant impact on the management of security strategies. It increases situational awareness, improves intelligence and surveillance capabilities, uncovers cybersecurity challenges, necessitates integration and interoperability, mandates training and skills development, and raises ethical and legal considerations. As a result, security managers should adapt to these changes to create robust and effective security strategies to counter evolving threats.

References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), 939-953.

Akçay, M. (2018). Teknolojik Değişimin Savunma Organizasyonlarında Yarattığı Yapı Değişikliği. Savtek 2018 Bildiri Kitabı, 1(1), 9.

Akyürek, S. (2012). İnsansız Hava Araçları:Muharebe Alanında ve Terörle Mücadelede Devrimsel Dönüşüm. İstanbul.

Alkan, C. (1998). Eğitim Teknolojisi. Ankara: Anı Yayıncılık.

Altın, Z. (2014). Türk Silahlı Kuvvetleri Teknoloji Yönetiminde Proje Performans Model Önerisi ve Örnek Olay İncelemesi. Kara Harp Okulu.

Astan, G. (2015). Gelişen Teknolojiler ve Değişen Muharebe Şartlarında Geleceğin Askerine Yönelik Teknoloji Öngörü Çalışması. Kara Harp Okulu.

Baldwin, D. A. (1997). The Concept of Security. Review of International Studies, 23, 5–26.

Baylis, J., & Smith, S. (2008). The Globalization of World Politics. Oxford: Oxford University Press.

Baysal, B., & Lüleci, Ç. (2015). Kopenhag Okulu ve Güvenlikleştirme Teorisi. Güvenlik Stratejileri, 11(22), 61–96.

Biscop, S. (2005), The European Security Strategy. A Global Agenda for Positive Power, Aldershot: Ashgate Publishing

Breschi, S., Malerba, F., Orsenigo, L., (2000). Technological regimes and Schumpeterian patterns of innovation. Economic Journal 110, 338–410

Bryce, J. (2001),The technological transformation of leisure, Soc Sci Comput Rev 19:7–16

Burtonshaw-Gunn, S.A. (2008). Essential Management Toolbox: Tools, models and notes for managers and consultants. Chichester, England: Wiley & Sons.

Buzan, B. (1991). People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. Boulder: Lynne Rienner Pub.

Chow, D. (2013). 7 Technologies That Transformed Warfare. Tarihinde 19 Ocak 2019, adresinden erişildi https://www.livescience.com/41321-military-war-technologies.html

Davelaar, E.J. and Nijkamp, P. (1990), Technological innovation and spatial transformation, Technological Forecasting and Social Change, Vol. 37, pp. 181-202

Dedeoğlu, B. (2004). Yeniden Güvenlik Topluluğu: Benzerliklerin Karşılıklı Bağımlılığından Farklılıkların Birlikteliğine. Uluslararası İlişkiler, 1(4), 1–21.

Demirel, Ö. (1993). Eğitim Terimleri Sözlüğü. Ankara: Usem YAyınları.

Drucker, Peter F (1974), Management: Tasks, Responsibilities, Practices. New York: Harper &

Row,

European Council (2003),European Security Strategy :A Secure Europe in a Better World, Brussels: European Council, 12 December

Erdoğan, F. A., Sağbaş, M., & Sundu, M. (2022). Yeni Nesil Harp Ortamında Askeri Liderlerde Olması Gereken Özelliklerin Bulanık AHP Yöntemi ile Önceliklendirilmesi. Social Sciences Studies Journal (SSSJournal), 8(102), 3181-3192.

Fontes, M. (2005), 'The process of transformation of scientific and technological knowledge into economic value conducted by biotechnology spinoffs,' Technovation, 25(4), 339–347.

Habertürk. (2017). En iyi insansız savaş araçları. Tarihinde 19 Ocak 2019, adresinden erişildi https://www.haberturk.com/ekonomi/savunma-sanayi/haber/1612791-en-iyi-otonom-savas-robotlari-insansiz-muharebe-donemi-basladi

Hamel, G. (2007). The future of management. Cambridge, MA: Harvard Business School Press.

Huysmans, J. (2007). Revisiting Copenhagen Or, on the Creative Development of a Security Studies Agenda in Europe. Europion Journal of International Relations, 4(4), 479–505.

İşman, A. (2014). Teknolojinin Felsefi Temelleri. Sakarya Üniversitesi Eğitim Fakültesi Dergisi, 0(1), 1.

Kellner, D. (2004). Technological transformation, multiple literacies, and the re-visioning of education. E-Learning, 1(1), 9-37.

Kendi, A. (2018). Yapay Zekâ ve Silahlı Kuvvetlere Etkileri.

Kohnová, L., Papula, J., Salajová, N. (2019), Internal factors supporting business and technological transformation in the context of industry 4.0 Bus. Theory Pract. 20, 137–145

Kott, A., Swami, A., & West, B. J. (2016). The Internet of Battle Things, 1–11.

Kumar, V. and Werner J. Reinartz (2006), Customer Relationship Management: Concept , Strategy and Tools, New York: Springer.

Lipschutz, R. D. (1995). On Security. New York: Columbia University Press.

Lister, J. (2017). The Impact of Technology on Warfare. Tarihinde 19 Ocak 2019, adresinden erişildi https://bizfluent.com/info-7844707-impact-technology-warfare.html

Magretta, J. (2002). What management is: How it works and why it's everyone's business. New York: Free Press.

Markard, J., and Truffer B. (2008), Technological innovation systems and the multi-level perspective: Towards an integrated framework. Research Policy 37: 596–615.

McSweeney, B. (1999). Security, Identity and Interests: A Sociology of International Relations. Cambridge: Cambridge University Press.

Meydan, C. H. (2015). Dünya Ordularında Yeniden Yapılanmanın Kaynakları Üzerine Bir İnceleme. Güvenlik Stratejileri, 21(1).

Oz, E. (2009), Management Information Systems. Cambridge, MA: Course Technology.

Öztürk, D. (2017). Technological transformation of manufacturing by smart factory vision: industry 4.0. International Journal of Development Research, 7(11), 17371-17382.

Pronoza, P., Kuzenko, T., & Sablina, N. (2022). Implementation of strategic tools in the process of financial security management of industrial enterprises in Ukraine. European Journal of Enterprise Technologies, 2(13), 116.

Rumelt, R. P., Schendel D., and Teece D. (1991), "Strategic Management and Economics," Strategic Management Journal, 12 (Winter), 5-30

Sandıklı, A., & Emekliler, B. (2014). 21. Yüzyılda Yeni Güvenlik Anlayısları ve Yaklasımları. Uluslararası Balkan Kongresi.

Skyrme, D. J. (2002), Developing a Knowledge Strategy: From Management to Leadership, In, (eds.) Morey, D., Maybury, M., and Thuraisingham, B, Knowledge Management: Classic and Contemporary Works. Cambridge, MA: MIT Press.

Snider, D.M. (1995), The National Security Strategy: Documenting strategic vision, 2nd edn.

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy. International Journal of Critical Infrastructure Protection, 2(3), 95-109.

STM. (2018a). Askeri Eğitimde Son Teknolojinin Kullanımı.

STM. (2018b). Uydu Savaşları.

Trim, P., & Lee, Y. I. (2022). Strategic cyber security management. Taylor & Francis.

Türk Dil Kurumu. (1988). Türkçe Sözlük. Türk Tarih Kurumu Basımevi.

Ural, Ş. (2016). Teknolojinin "Teknoloji" Kavramı ve Değerlerle İlişkisi. Yeni Türkiye Dergisi, 88(1), 295–302.

van de Poel, I. (2003), The transformation of technological regimes, Research Policy 32 (1):49-68

van den Ende J and Kemp R (1999), Technological transformations in history: How the computer regime grew out of existing computing regimes. Research Policy, 28: 833–851.

Vellani, K. (2006). Strategic security management: a risk assessment guide for decision makers. Elsevier.

White House (1991), A National Security Strategy of the United States, Washington, DC: The White House

White House (1998), A National Security Strategy for a New Century, Washington, DC: The White House

White House (2010), National Security Strategy. Washington, DC: The White House (May).

White House (2017), National Security Strategy. Washington, DC: The White House

yeniisfikirleri.net. (2018). Nesnelerin İnterneti (Internet Of Things) Nedir? Örnekleri Nelerdir? Tarihinde 20 Ocak 2019, adresinden erişildi http://www.yeniisfikirleri.net/nesnelerin-interneti-nedir-ornekleri-neler