ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/381846870

The concept of smartwar: A theoretical framework

Article · June 2024

CITATIONS
0

READS
93

2 authors, including:



Aslıhan Ünal
Gelişim Üniversitesi
31 PUBLICATIONS **114** CITATIONS

SEE PROFILE

All content following this page was uploaded by Aslıhan Ünal on 30 June 2024.

The user has requested enhancement of the downloaded file.

Nosyon: Uluslararası Toplum ve Kültür Çalışmaları Dergisi - Nosyon: International Journal of Society and Culture Studies 2024, 13, 35-57

The concept of smartwar: A theoretical framework

Orkun Öz[*], Aslıhan Ünal[**]

Abstract

With the exponential developments in information technologies "Smart" as a one-size-fits-all has become a popular term nowadays in literature and media. Smartphones, smart watches, smart devices, smart technology, smart weapons, and smart war… Besides, these developments have given rise to the debate as "Has the concept of war been changed?", "What does smart war mean to humanity?", "What are the benefits and risks of artificial intelligence-based technology in warfare", "What is the type of war humankind experiences today?", "Has the dynamics of war changed?", etc. Hence, the advances in technology have started to influence the nature of war. Although the term "smart war" become popular, it is realized that a few studies have been conducted on this concept. There are many studies on artificial intelligence in warfare, electronic warfare, autonomous weapon systems, drones, smart weapons, unmanned aerial vehicles (UAVs), robot soldiers, etc. but a gap in the literature is the lack of a comprehensive work that examines the similarities of the conflicts in terms of strategies, weapons, and actors in the age of IT. This study is conducted to fill this gap in the literature. The purpose of this study is to examine modern conflicts that arise with the exponential developments in IT and put forward a theoretical framework that explains the smart war concept. For this purpose, the answer to the research question "How can the smart war concept be defined?" was examined by adopting an exploratory approach and following grounded theory methodology. As a result, a theoretical framework that explains the smart war concept in four dimensions -antecedents, actors, technologies, and strategies introduced. Further, the framework was evaluated through real-world cases of conflict.

Research article
Geliş - Submitted: 11.05.2024
Kabul - Accepted: 12.06.2024
Atıf – Reference: *Nosyon: Uluslararası Toplum ve Kültür Çalışmaları Dergisi*, 13, 35-57.

Keywords: Smart war, information technology, artificial intelligence, modern war, grounded theory

Akıllı savaş kavramı: Teorik bir çerçeve

Öz

Bilgi teknolojilerinde yaşanan üstel gelişmelerle birlikte "akıllı" kelimesi günümüzde literatürde ve medyada popüler bir terim haline gelmiştir. Akıllı telefonlar, akıllı saatler, akıllı cihazlar, akıllı teknoloji, akıllı silahlar ve akıllı savaş... Ayrıca bu gelişmeler "Savaş kavramı değişti mi?", "Akıllı savaş insanlık için ne anlama geliyor?", "Savaşta yapay zeka temelli teknolojinin faydaları ve riskleri nelerdir?", "İnsanlığın bugün deneyimlediği savaş türü nedir?", "Savaşın dinamikleri değişti mi?" gibi tartışmalara da yol açmıştır.Dolayısıyla, teknolojideki ilerlemeler savaşın doğasını da etkilemeye başlamıştır. "Akıllı savaş" terimi popüler hale gelse de bu kavram üzerine çok az çalışma yapıldığı görülmektedir. Savaşta yapay zeka, elektronik savaş, otonom silah sistemleri, insansız hava araçları (İHA), akıllı silahlar, robot askerler vb. konularda pek çok çalışma bulunmakla birlikte, bilişim çağında çatışmaların strateji, silah ve aktörler açısından benzerliklerini inceleyen kapsamlı bir çalışmanın bulunmaması literatürde bir boşluk olarak belirlenmiştir. Bu çalışma, literatürdeki bu boşluğu doldurmak için yapılmıştır. Bu çalışmanın amacı, bilişim teknolojilerindeki üstel gelişmelerle birlikte ortaya çıkan modern çatışmaları incelemek ve akıllı savaş kavramını açıklayan teorik bir çerçeve ortaya koymaktır. Bu amaçla, "Akıllı savaş kavramı nasıl tanımlanabilir?" araştırma sorusunun cevabı keşifsel bir yaklaşım benimsenerek ve gömülü teori metodolojisi izlenerek incelenmiştir. Sonuç olarak akıllı savaş konseptini dört boyutta açıklayan

* Bir kurama bağlı değil, e-posta: orkun_oz@hotmail.com, ORCİD ID: 0000-0003-0855-1635
** Sorumlu yazar, Dr. Öğr. Üyesi, İstanbul Gelişim Üniversitesi, İktisadi İdari ve Sosyal Bilimler Fakültesi, e-posta: asunal@gelisim.edu.tr, ORCID ID: 0000-0001-5896-8880

teorik bir çerçeve ortaya konulmuştur: Öncüller, aktörler, teknolojiler ve stratejiler. Ayrıca, geliştirilen çerçeve, gerçek dünyadaki çatışma vakaları üzerinden değerlendirilmiştir.

Anahtar Kelimeler: Akıllı savaş, bilişim teknolojisi, yapay zeka, modern savaş, gömülü teori

Introduction

With the rise of machines and the Internet in the information age and groundbreaking developments in artificial intelligence (AI) technology, “smart” has become a catchall term in our lives, especially used to define a phenomenon that assists or takes over work as smartphones, smartwatches, and smart cities and supports wiser decision-making as smart energy, smart strategy, and smart war. The emergence of information technology (IT) and the foundation of AI as a scientific discipline triggered the rise of the concept of "smart,” and with the promotion of personal computers, the commercialization of the Internet, and the appearance of mobile phones, the “smart” phenomenon started to diffuse in our everyday lives, and the media also promoted this invasion. The exponential development of IT (see “Moore Law”) has been fostering a paradigm shift and has had a destructive impact on how we experience the world. The war practices and the literature have also been influenced by this attack, and the “smart war” concept eventually appeared in the scientific papers alongside the media sources. Actually, “smart war” is not a brand-new term, and it has been used in the literature since the 1990s. At that time, the term was associated with the Gulf War according to the notions that support technological developments, which decreased the level of violence. For example, John Carlos Rowe (1991) used the term to distinguish the Gulf War from the Vietnam War:

> However the public discussion of such crucial issues of democratic governance depended to a large extent on remembering what was the continuing legacy of Vietnam. And it was precisely this sort of cultural memory that the decisive military victory in the Gulf helped to erase. The Persian Gulf War was mercifully swift and relatively bloodless for the Coalition's forces. The "Vietnam without trees" that some antiwar activists had predicted never came to pass in the desert along the Gulf. We have been encouraged to believe a "clean," "sanitary," and "smart" war was the result of the superior technology, organization, and justness of the Coalition's leaders, both in the field and in Washington. As Kuwaiti Coalition troops led the way into Kuwait City, to be met by resistance fighters, and as U.S. forces swept into southern Iraq, driving Iraqi troops across the Euphrates or into Basra, the fears of another Vietnam vanished (Rowe, 1991, p.123).

Michael N. Schmitt (1999) also used the term by referring to the Gulf War; furthermore, he defined it as the “first smart war”:

> Complementing the revolution in information systems are equally impressive advances in weapons capabilities. Inaccurately hailed as the first "smart" war,' the 1991 Persian Gulf War popularized the capabilities of precision-guided munitions. Though the accuracy and effectiveness of smart weapons in that war may have been exaggerated through coverage in the popular media, the weapons of future wars will be more than smart-they will be "'brilliant" (Schmitt, 1999, p.164).

Besides, Roger Normand (2001) mentioned in his article that the Gulf War was approved as a “smart war,” although it was not. Hence, attention turned from ‘The Iraqis would not be injured’ to ‘the success of smart bombs thanks to their ability to accurately target.’ William M. Arkin (1992) handled the term associated with the cruise missiles used in the Nobel Anvil operation of NATO against Yugoslavia:

> After more than two months of bombing, the day-in-day-out use of the B-2-and its B-1 cousin was the only militarily significant technological development of an otherwise miserable war. Modern intercontinental bombers had joined a prolonged “smart” war; the era of unmanned cruise missiles had been eclipsed; America was launching bombers from its own soil (Arkin, 1992, p. 80).

Hodge (2000) handled the smart war concept as a kind of war that avoids casualties by using smart weapons such as target-sensitive bombs, missiles, etc., and pointed out the first

evidence of the smart war that has the potential to lead to casualties as the USA's missile attacks against Afghanistan and Sudan. Kate Farris (2000) used the term as synonymous with "information war" and examined it from the lens of China and the USA's practices and strategies. The author defined information warfare by focusing on IT and not limiting the concept to "smart bombs" or "missiles":

> We hold that information warfare has both narrow and broad meanings. Information warfare in the narrow sense refers to the US military's so called 'battlefield information warfare,' the crux of which is 'command and control warfare'… Information warfare in the broad sense refers to warfare dominated by information in which digitized units use information [smart] equipment... (Farris, 2000, p. 9).

In the 2010s, the concept evolved with the rise of IT and covered a wide range of weapons based on emergent technologies. For example, Crispin Andrews' (2012) article titled Smart Warfare starts with the prologue "The development of aerial drones, smart bullets, and laser guns all point to a future of global conflict resembling science fiction". Although the author did not use the term "smart warfare" throughout the article except in the title, he focuses on emerging technologies such as aerial drones, unmanned aerial vehicles (UAVs), and smart bullets and highlights the importance of information gathering, especially emphasizing its crucial role in future warfare. In 2020, the smart war concept is built on based on artificial intelligence and associated technologies such as the Internet of Things (IoT), blockchain technology, advanced data analytics, cloud computing, robot soldiers, swarm intelligence, etc. (e.g., Hocaoğlu & Genç, 2019; Qi, 2021). In the war literature, the smart war concept covers a wide range of research areas, such as electronic war, information war, smart strategy, drone war, automated weapon systems, smart soldiers, artificial intelligence-based weapons, etc. It is also used outside of the military to define a fight against a phenomenon. For example, Pathak et al. (2019) used the term "smart war" to describe the fight against the COVID-19 pandemic by using digital technologies. It is clear that the root of the concept lies in emergent technologies, but the definition of it is not clear, and its theoretical underlying is vague. It has been used as an umbrella term that covers the evolution of the war concept in modern times. Many studies cover the use of IT in warfare, but the gap in the literature is the lack of comprehensive work that examines the similarities of the conflicts in terms of strategies, weapons, and actors in the age of IT. This study was conducted to fill this gap in the literature.

The purpose of this study is to examine modern conflicts that arise with the exponential developments in IT and put forward a theoretical framework that explains the smart war concept. For this purpose, the answer to the research question "How can the smart war concept be defined?" was examined by adopting an exploratory approach and following grounded theory methodology. As a result, a theoretical framework that explains the smart war concept in four dimensions—antecedents, actors, technologies, and strategies—is introduced. Further, the framework was evaluated through real-world cases of conflict.

The article proceeds as follows: At first, the methodology of the research—grounded theory— is explained. Then, the findings of the research—the theoretical framework and smart war definition—are presented. Afterward, the concept of smart war is evaluated through real-world examples. In the final section, a general overview is introduced with theoretical implications, and recommendations for future research are provided.

1. Methodology

An exploratory research design, grounded theory, was followed to establish the theoretical framework of the concept of smart war. Grounded theory was discovered by Barney Glaser and Anselm Strauss (Glaser & Strauss, 2017) and was first used in the field of sociology to develop data-based theories. In later periods, different application designs were developed,

and it started to be used as an exploratory methodology in various research fields and also in standalone literature review research (Wolfswinkel et al., 2011). In this research, the grounded theory design was preferred to examine and found the theoretical framework of the ambiguous “smart war” concept.

In grounded theory research, any kind of material can be used as data. In this study, in addition to academic literature, any written and visual source (e.g., blog posts, newspaper articles, YouTube videos, etc.) that is believed to contribute to the concept of smart warfare has been used. The data were collected and analyzed simultaneously, following the theoretical sampling method. A theoretical model explaining the concept of smart warfare was developed by following an analytical coding process (initial coding, axial coding, and selective coding) (Wolfswinkel et al., 2011).

In grounded theory research, sample selection, data collection, and data analysis processes are carried out in an intertwined manner. In the initial stage of the research, a search was conducted using the keywords "smart war" and "smart warfare" in the Web of Science (WoS) and Google Scholar indexes to reach the definition of smart war. As a result of the WoS database search, one article and one conference paper were accessed (see Sample 2003; Imran et al., 2018). Google and Google Scholar search several sources by using the keyword "smart war". It was determined that the concept of "smart war" is approached from different perspectives in academic publications and other internet sources. For example, the concept of smart war has been associated with artificial intelligence-based weapon systems (e.g., Preußger, 2023), soft strategy (e.g., Rosenberg, 2013; Simons, 2012), wars that yield minimum costs and maximum success (e.g., Warden, 2008), unmanned missiles and bombs (e.g., Arkin, 1999; Hodge, 2000), robotics (e.g., Imran et al., 2018), systems consisting of sensors, C3I (Command, Control, Communication, and Intelligence), and precision-guided munitions (e.g., Yeon-Bong, 2019).

For example, Image 1 shows a LinkedIn post titled “Smart War?" shared by a graphic artist named Manuel Alvaroz Junco. In the display, the head of a man in a suit is replaced by a missile, and the background shows bombed areas with these missiles. The image can be interpreted as representing a war in which "smart" weapons are a product of human mental processes, but humans are not physically involved in the process. Hence, it can be said that the image represents smart war as a type of war controlled by "mind teams" or "higher intelligence".

Image 1. An illustration of the smart war



Source: Alvarez-Junco, M. (2022). Smart war?. LinkedIn.

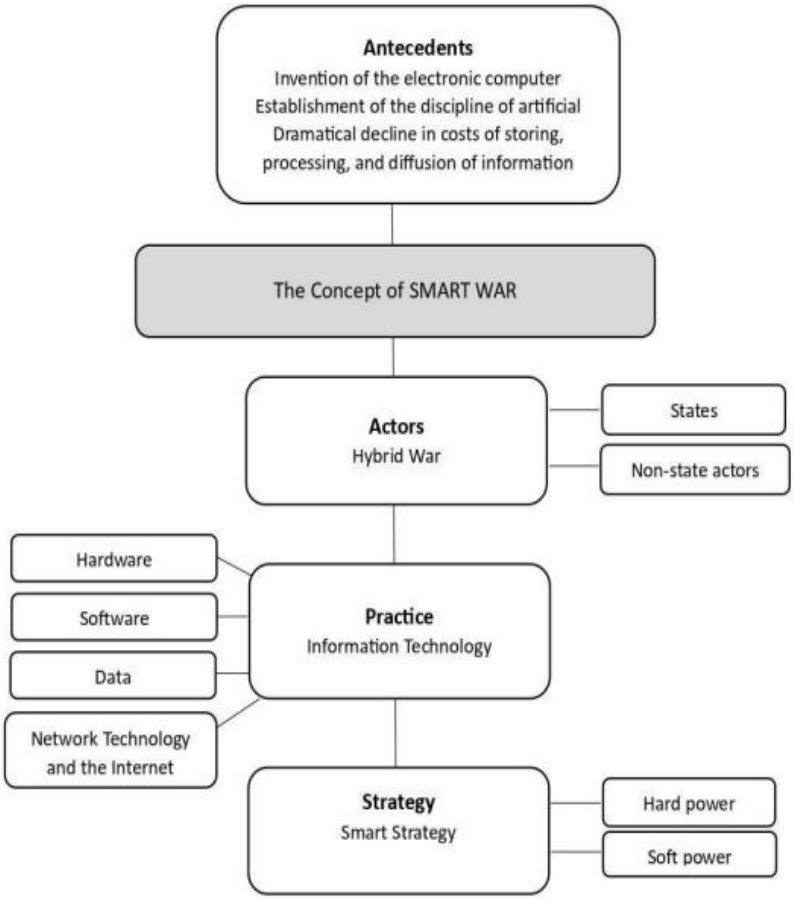
There is a notion that humans are removed from the death chain physically thanks to smart weapons (drones, smart bombs, missiles, etc.), and targeted killings provide more accurate results and decrease unplanned deaths (Yan, 2020). In most of the examined sources, it was found that the smart war concept primarily emphasizes the automation of weapons and the mental participation of humans. However, it was defined that there was no common definition for this new type of warfare that has evolved parallel to advancements in information technologies.

In this study, keywords such as "information warfare", "electronic warfare", "autonomous weapons", "electronic weapon systems", "artificial intelligence", "smart strategy", "hybrid warfare" and similar words were used to enrich the data set. Common features that would define the concept of smart war were searched for in the written and visual data. Once a theory emerged, document analysis was used to find and test examples that could be explained by the theory. The authors' expertise in political science and management information systems helped to maintain a transdisciplinary perspective in the development of the theoretical framework. The authors' previous areas of work and the sources they have examined have influenced the references.

2. Theoretical framework of the smart war concept

As a result of the grounded theory process, the theoretical framework presented in Figure 1 was developed.

Figure 1. The theoretical framework of the smart war concept



The theoretical framework comprises four categories: 1) antecedents, 2) actors, 3) applications, and 4) strategies. Antecedents mainly include developments that emerged during the Second World War and the Cold War period. Actors are assessed from the perspective of hybrid warfare, which includes both state and non-state actors involved in smart warfare. Applications include types of weapons that use different components of IT. "Strategies" deals with the smart strategies that are used to achieve desired goals through the use of IT. The above categories are discussed in detail in the following sections.

2.1. Antecedents of smart war

World War II and the Cold War were periods in which the foundations of IT were laid, and new types of warfare based on this emerged. The remarkable developments in the field of technology that occurred during and immediately after World War II played a crucial role in the transition from the Cold War era to the era of smart warfare. The foundations of still developing technologies such as the internet, computers, and artificial intelligence were laid during this period.

In his article titled “On Computable Numbers with an Application to the Entscheidungsproblem”, Alan M. Turing (1937) laid the theoretical foundations of computer science by explaining how the universal Turing machine (modern computer) should operate. Turing also played a crucial role in shortening World War II by approximately 2 years by decrypting the Enigma code used by the German military forces to communicate (Robinson 2014). The ENIAC, developed in 1946, was the first electronic computer that operated according to the universal Turing machine (Goldstine & Goldstine, 1946). The purpose of developing the ENIAC was to calculate ballistic firing tables during World War II (Weik, 1961).

The idea of connecting computers originated from the need for the Soviets to develop a defense system against air attacks during the Cold War. The efforts to develop air defense radar technology due to the threat posed by nuclear weapons played a triggering role in the emergence of the Internet. ARPANET, developed with the support of the US Department of Defense (DoD), was created to take precautions against nuclear threats, ensure control of US nuclear forces, and improve military tactics and management decisions by utilizing new computer technologies (Lukasik, 2011). DARPA was established for conducting such research and development activities, and in 1969, the first internet-like connection was established through ARPANET via four main centers (Perry et al., 1988). As a result, ARPANET considered the precursor to the Internet, began to be used more widely.

The Cold War has also led to significant funding for research on machine translation (automatic language translation). Oettinger, a student at Harvard University, is one of those involved in Russian-English translation projects (Daylight, 2015). Another striking development during this period was Alan Turing's (1950) article Computing Machinery and Intelligence, which brought a new perspective to the concept of a “thinking machine” and introduced the Turing Test. In the Turing Test, which is the machine-human version of the imitation game, the machine, and the human are evaluated based on the answers they give in the text, and it is guessed which one is human and which one is a machine. If the machine can convince the evaluator that it is human, then that machine can be considered intelligent (Turing, 1950). The Turing Test caused a great impact at that time, and shortly after, at the Dartmouth Conference organized by McCarthy and his colleagues in 1956, the term "artificial intelligence" was used for the first time, and artificial intelligence was established as a scientific discipline (Moor, 2006). The studies on artificial intelligence started with the assumption that a machine capable of imitating all aspects of human cognitive abilities could be created (McCarthy et al., 2006). This goal has not yet been achieved until today. In the following periods, artificial intelligence, which has been divided into various subfields, has

achieved victories by exhibiting superhuman intelligence in limited areas, although not in the general field. Artificial intelligence applications used in the military, business world, and social fields today are examples of narrow artificial intelligence.

In addition to these developments, space has become one of the biggest competitive areas of the Cold War. Both countries allocated large budgets for space competition. During this period, the Soviet Union succeeded in placing the first man-made satellite, Sputnik, into space. In response, the US became the first state to send humans to the moon with the landing of Apollo 11 (History.com, 2020). During the same period, ARPA.NET, the precursor of the internet, developed a nationwide network on decentralized servers against a possible Soviet nuclear attack.

2.2. The actors of smart war

In literature, wars are traditionally classified as interstate and intrastate from the perspective of actors. Non-state actors are also included in this classification. Non-state actors can initiate wars against states, and states can initiate wars against non-state actors, or non-state actors can have conflicts among themselves. For example, civil war, guerrilla warfare, riots, and people's war are subsets of intrastate wars known as "asymmetric warfare" (Kiss, 2014; Thornton, 2007). In hybrid warfare, there are no sharp classifications like states and non-state actors. For example, combining the high-tech weapons of states with cyberattacks targeting terrorism and financial goals is an example of hybrid warfare (Hoffman, 2009). Suicide bombings by illegal organizations, propaganda campaigns, and manipulation actions on social media can also accompany these actions. The actor in such actions can be an individual or a group formed by the combination of many civil society organizations. When various examples are examined in this regard, it can be seen that smart warfare overlaps with hybrid warfare from the actors' perspective.

Hybrid war is a type of war implemented by non-state and state actors, that involves unconventional conflicts such as terrorism, violence, chaos creation, cyber warfare, media, and economic practices, along with conventional military capabilities and tactics (Josan & Voicu, 2015). Although the concept of hybrid warfare emerged in the mid-2000s in the US military and gained attention with Russia's annexation of Crimea, various tools such as information war, proxy war, sabotage, and psychological operations have been used by armies long before (Renz, 2016). Gathering information to understand both one's own and the enemy's strengths and weaknesses can be traced back to the ancient strategy book, The Art of War (5th century BC), which includes the following words of Sun Tzu (Tzu, 1963):

> 31. Therefore, I say: 'Know the enemy and know yourself; in a hundred battles you will never be in peril.
> 32. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal
> 33. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril.'

The concept of smart war, which is the subject of this article, is based on information technology, so it would be correct to say that this new type of warfare carries traces to the first half of the 1900s instead of being based on a specific start date or event.

The similarities between the concepts of smart war and hybrid war are the use of both conventional and unconventional weapons, the involvement of state and non-state actors, or a combination of both, as actors. Unconventional operations such as political protests, cyberattacks, disinformation attacks, and manipulation can accompany conventional and irregular operations (Wither, 2016). Through capitalism, the commercialization of advanced weapons increases the lethality level of non-state actors (Yan, 2020). At the same time, these powers, through advancements in information technology, can compete with states in shaping public opinion, as non-state actors can influence public opinion (Wither, 2016).

2.3. The practice of smart war

Smart war can be considered a war based on IT and is conducted in collaboration between humans and machines. To better understand this collaboration, it is necessary to define concepts such as data, information, and information systems that are related to each other. Data can be defined as independent and contextless symbols that are obtained through observation and measurement methods and do not become meaningful without processing. Processed, organized, and meaningful data is called information (Ackoff, 1989). Data becomes meaningful information for humans by processing and correlating it (Laudon & Laudon, 2022). Information technology (IT) is a series of interconnected components that collect, process, and distribute information in an organization to facilitate decision-making and control. In summary, data entering information systems is transformed into information through processing. According to Bourgeois et al. (2019), an information system is a concept that encompasses the components of the system and their roles within the organization. Software, hardware, data, network communication, people, and processes are the fundamental components of an IT system. The first four of these components are technology components. The other components ensure the integration of the system into the organization. The four main components of information systems are shown in Table 1.

Table 1. Components of information systems

Components of Information System	Hardware	Hardware is the physical part of the system. It includes digital technology components. Desktop, laptop, tablet, smartphone, and other digital devices and their physical parts are examples of hardware. Internet of Things (IoT) technology enables data flow and communication between devices through sensors and receivers.
	Software	Software is a series of instructions that operate the hardware. It is divided into two categories: operating system and application software. The operating system manages the hardware and creates an interface between the hardware and the user (Windows, MacOS, Android, etc.). Application software performs specific tasks such as word processing, accounting, database management, gaming, presentation preparation, etc.
	Data	Data is an unprocessed fact. It has no context and is not organized for a purpose. Data is transformed into information through processing. Information is created by organizing data according to a specific purpose and putting it into context. Knowledge is the human belief and perception that is formed about the relationships between concepts and findings in a specific field. Big data refers to large volumes of data that traditional data processing technologies are inadequate to handle. It can consist of structured, semi-structured, or unstructured data. Data is organized and stored in a database. Relational databases are the most used type of database. Database management systems are used in the creation and management of databases. A data warehouse is a special type of database that retrieves and analyzes data from another database. Data mining techniques are used in the processing of data. Data mining enables the discovery of relationships and patterns within large data sets. Many organizations use data management technologies to convert data into actionable information (business intelligence) and gain competitive advantage.
	Network technology	Network technology (intranet, extranet, Internet, www, and wireless access) connects computers, enabling access to information and the dissemination of information. Cloud computing technology has made it possible to access information from anywhere. As a result, businesses or individuals can store data on the internet and use applications provided through the cloud.
	Human	People at every level of an organization who use information technologies are an important part of information systems. People

	Process	imagine, develop, support, and most importantly, use information systems. The process is a series of steps followed to achieve a goal or obtain an output. In short, it can be expressed as the transformation of input into output. Document management systems, enterprise resource planning systems, and information systems are dependent on organizational processes. Organizations that successfully manage this integration gain competitive advantage.

Source: The table was formed by the authors according to Bourgeois, D. T., Smith, J. L., Wang, S., &Mortati, J. (2019). Information Systems for Business and Beyond. Open Text Books.

The components of the information system shown in Table 1 play an important role in defining the concept of smart war. The concept of smart war examined in this article corresponds to a war where information systems, i.e., human and machine collaboration, are at the center. Therefore, the history, technologies, and strategies of the smart war are related to information systems. Various components of information systems can be used as weapons in smart wars. Examples of these weapons are evaluated based on the five dimensions of hybrid war in Table 2.

Table 2. Smart war weapons

Dimensions	Weapons	Examples
Military	*Autonomous weapons* C4ISR2 - Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR). *Fast and accurate automatic target recognition systems*	Automatic target recognition systems (ATR) developed by DARPA
Political	*Social media* *Deepfake videos and audios* Disinformation Propaganda Manipulation	Attempts by Russia to blur the line between reality and fiction, divide and separate through automatic (bots) and anonymous accounts on social media, and undermine the reputation of institutions of the West. Influencing public opinion in internal elections through machine learning methods. Attempts to manipulate psychological manipulation and change voting decisions by using social media users' data through Cambridge Analytica during the 2016 US elections.
Economic	*Physical and cyber attacks* Causing damage to the economic infrastructure Launching cyber-attacks on financial centers and networks. Creating disorder, deterioration, financial collapse, and social chaos in the economy in this way.	Attacks by Anonymous Hack Group to the official websites of Russian institutions during the Ukraine-Russia war.
Civil	*Artificial intelligence* *Social media* *Digital propaganda* *Deepfake videos* Mobilizing civil society, creating a chaotic environment, manipulation Exploiting religious, sectarian, and ethnic groups with realistic videos created by artificial intelligence	Arab Spring American comedian Jordan Peele's fake video of mimicking Obama and making him say desired words.

Informational	Fake terrorist attack videos *Artificial intelligence* *Bots* *Search engines* *Generating fake content* Producing fake news content accompanied by realistic video and audio recordings, Preventing access to real content through large-scale information flow attacks with the help of bots, covering it up, Manipulating access to information by influencing user behavior through search engines.	In 2016, a competition called Cyber Grand Challenge was organized by DARPA, where programs that could automatically defend themselves while attacking competitors were produced.

Source: The table was produced by the authors according to Yan, G. (2020). The impact of artificial intelligence on hybrid warfare. *Small Wars & Insurgencies, 31*(4), 898-917.

3.4. Smart war strategies

When considered at the country level, defense strategies can be classified as "hard power" and "soft power" and as “written (official) strategies” and “unwritten strategies”. The distinction between hard power and soft power is related to the type of power applied to achieve the desired outcome. According to Joseph Nye (2023), smart power is an intelligent combination of hard and soft power tools such as diplomatic networks, defense, development, etc., and power is the ability to influence others to achieve desired outcomes. Others' behavior can be influenced in three ways (Nye, 2019): (1) coercion, threats of force, (2) incentives and payments, and (3) attraction and persuasion for others to do what you want. The first two options represent hard power. Those who can achieve what they want by using soft power, which can be effective with the ability to attract and persuade, can save on more options that require soft power. To obtain soft power, civil society, and diplomacy based on trust and friendly communication are required. The information revolution we are experiencing today has changed the nature and spread of power. Technological developments subject to Moore's Law have dramatically accelerated the collection, storage, processing, and dissemination of information. This revolution, which is synonymous with the popular saying "data is the new oil" impacts a wide range of areas, from states to individuals that require soft power. Soft power has entered our homes with mobile phones today and offers the ability to influence the global agenda, even for a single individual. The smart strategy is to be able to apply the optimal combination of hard and soft power.

The creator of the concept, Nye (2009), states that the knowledge of how hard and soft power sources can be combined is related to contextual intelligence. Contextual intelligence is the intuitive diagnostic ability that helps create intelligent strategies by aligning tactics with goals. Soft power is an important tool to dominate the masses, but in some cases, soft power alone is not effective, and intervention with hard power is necessary. Nye (2009) explains this concept through the following examples: Military intervention was necessary to disrupt the cooperation between Hamas and Al-Qaeda, or Kim Jong-Il would not end his nuclear weapons program by watching Hollywood movies. Soft power offers longer-term and broader effects. For example, in cases such as the protection of human rights, the development of civil society, and the improvement of democracy, the use of public diplomacy is more appropriate than the use of military power and coercion. The context of war plays a key role in determining the strategy in smart strategy.

Advancements in information technology contribute to both hard and soft power in smart strategy. Artificial intelligence-supported weapons, drones, UAVs, robot soldiers, and

even cyber-attacks are used to increase the hard power of state and non-state actors. Tools such as the Internet, social media, video content platforms, etc. are highly effective in creating soft power. When creating a smart strategy, the current situation can be analyzed most appropriately, and the combination of these two strategies can be applied. According to Nye (2023), a country's strategy (grand strategy) is the theory and stories related to ensuring the country's security, defense, and welfare reflect the identity of its leaders, and this strategy should be adjustable according to the context. The capitalist economic system enabling the commercialization of technology leads to conflicts between states, groups supported by states, or groups fueled by personal resources, becoming even more deadly.

Examples of the implementation of smart strategy can be given, such as the annexation of Crimea by Russia in 2014 and the Hezbollah-Israel conflict in 2006. The use of advanced weapons and communication systems by Hezbollah, supported by Iran, and the dissemination of information through the internet and media tools have surpassed Israel's success in influencing global public opinion since the beginning of the conflict (Wither, 2016). The Israeli attacks targeting civilians that started on October 7, 2023, have reversed the sympathy of the global public in favor of Palestine, paving the way for Israel to use hard power. In this regard, Chang (2023) has proposed the use of GPT-4, supported by ChatGPT, which works on large language models (LLMs), to resolve the ongoing historical dispute between the two countries. In the study, a discussion was designed in which two GPT-4 agents (Agent A and Agent B) sought a solution to the Israel-Palestine issue. The human role is minimal as a moderator in the 4-round discussion. As a result, Agent A proposed 10 arguments in each round that a solution is possible, and Agent B proposed arguments that it is not possible, and the moderator (author) made inferences based on these arguments. The result is that negotiations alone are not sufficient, and the conflict is "not yet" resolvable. This study gives the impression that a conflict-free environment can evolve through mutual arguments where smart war is discussed. Considering that Chat GPT-like LLMs are trained with human data, the importance of soft power becomes even more apparent. In today's global information sphere, victory sometimes depends not on whose army wins but on whose story wins. Public diplomacy and the ability to attract and persuade are effective in this regard (Nye, 2019).

The implementation of a soft power strategy can vary depending on the understanding of the parties involved. For example, China follows a more aggressive and proactive foreign policy against unfair attacks with its "Wolf Warrior Diplomacy". Diplomats and spokespersons effectively use social media to counter these attacks (Zhu, 2020). Especially during the COVID-19 pandemic, state-sponsored bot accounts have been used to counter criticisms against China (Blomquist, 2022).

2.5. The concept of smart war

The concept of smart war can be defined as follows based on the theoretical framework presented.

Smart War is a type of war that involves state and non-state actors, triggered by developments in information technology, where components of information technology are used as weapons and aim to gain superiority over the enemy by following a smart war strategy**.**

The elements that constitute this concept are summarized in Table 3.

Table 3. Components of Smart War

Components	Explanations	Examples
Antecedents	Information is a tool that has been used in wars since ancient times. The concept of smart war is based on information technology, so it can be said that the	Invention of the electronic computer The invention of the internet

	emergence and development of this type of war progresses parallel to the emergence and development of information technologies. Especially World War II and the Cold War are the periods in which factors influenced the concept of smart war.	Advancements in information technology Significant decrease in the cost of storing, processing, and distributing information Increase in communication speed
Actors	Smart war is similar to hybrid war in terms of actors and tactics. The regular armies of states, state-supported groups, illegal organizations or units, and even personal initiatives or groups formed by the combination of these actors can be the parties of smart war.	Annexation of Crimea by Russia Israeli-Palestinian conflict Cyber attacks Suicide bombings
Practices (Technologies)	Smart war practices use information technology as a tool. Information technology components (hardware, software, data, network technology) can be used as weapons in creating hard power and soft power.	Drones UAVs AI robots Social media Internet Bot accounts
Strategies	Being successful in smart warfare depends on being able to create and implement smart strategies. A smart strategy consists of an optimal combination of hard power and soft power. The proportion and way these two powers are used are related to contextual intelligence.	Propaganda Public diplomacy Friendly relationships Coercion and use of force Payments Disinformation

3. Smart war cases

In this section, the theoretical framework of smart war is evaluated through real-world cases. The following criteria considered in selecting sample cases.

1. Date: Mid-20th century-today
2. Actors: state, non-state, individuals, organizations, or a group of people
3. Practice: conventional and unconventional methods, but especially IT should be involved in the process
4. Strategies: Hard and soft strategies
5. Intriguing and unusual cases to attract the audience’s attention.
6. Support theoretical framework.

3.1. USA-China competition

The United States and China, the two biggest actors in the smart battlefield, are engaged in fierce competition. These two countries, which are pioneers in technology, continue their struggle in every aspect of smart warfare, and the race to be at the forefront intensifies this competition even more. One of the areas of competition between these two countries is the chip industry. Recent developments in the chip industry, which has critical importance in this field, have brought this competition to the forefront. The US Congress has approved the "Chip and Science Act of 2022" which provides a $280 billion incentive for domestic chip production on July 27-28, 2022 (National Science Foundation, 2023). According to the law, companies that want to benefit from the incentive are required not to improve the technological capacity of their facilities in China. Similarly, the Industry and Security Bureau affiliated with the US Department of Commerce implemented regulations consisting of restrictions on Chinese manufacturers' access to advanced chip technologies on October 7, 2022 (Aytekin, 2022).

One of the most important fronts of the smart war between the two countries is Huawei Technologies Co. Huawei, which operates in 170 countries and works with many of the world's important telecommunications companies, is a company located at the center of

China's artificial intelligence and 5G technology. Being the leader in 5G technology, which has approximately 1 billion users, will provide a significant advantage in global power competition. To prevent this advantage for China, the US is demanding a ban on equipment belonging to Huawei company from countries that are NATO allies under the intelligence alliance called Five Eyes Alliance (Akçay, 2020). In the face of these developments, China has imposed restrictions on the export of gallium and germanium, which are important raw materials in chip production. With this decision, which came into effect on August 1, 2022, approval from the relevant authorities is required before exporting gallium and germanium (Günyol & Yılmaz, 2023).

In addition to these, artificial intelligence technology is also one of the biggest areas of competition between the two countries. At the end of 2022, OpenAI introduced the ChatGPT model, a conversation bot based on Large Language Models (LLMs) (OpenAI 2022), and met with great interest worldwide. In order not to fall behind in this competition, Alibaba Group and Alibaba Cloud Intelligence announced TongyiQianwen in April 2023, a system trained on a large amount of data (Alibaba, 2023). Another technology giant in China, Baidu, has announced the release of its artificial intelligence chatbot service called Ernie Bor (Kharpal, 2023).

On the cyber-attack front, both countries have developed effective cyber action defense strategies. In this regard, the US announced its Cybersecurity Strategy on March 3, 2023, (The White House, 2023). China and Russia are the countries posing the greatest cyber threats to the US in this strategy. The aim is to create a resilient and defensible digital world to prevent domestic or foreign hacker activities. The same report also includes mandatory regulations within the scope of cybersecurity. Another notable part of the report is that it authorizes retaliation against cybercrime networks and attacking country governments' computer networks in response to cyber-attacks on American networks by defense intelligence and law enforcement forces. The Biden administration has stated that cyber defense has been carried out so far through the efforts of individual users and small groups. However, this situation is far from the desired level in terms of cybersecurity. Therefore, it emphasizes that public institutions, military law enforcement forces, and other military institutions should also take responsibility in this regard. According to the report, the biggest attacks in recent years are the takeover of the SolarWinds Orion network by Russian hackers and the attempted takeover of Microsoft Exchange servers by groups believed to be of Chinese origin. According to the report, the burden of cybersecurity should be shifted from individuals, small businesses, and local governments to specialized areas (The White House, 2023). In line with this report, the Department of Defence (DoD) has published the Cyber Workforce Strategy Implementation Plan covering the years 2023-2027 (DoD, 2023). Mark Gorak, Chief Information Officer (CIO), stated that they have created a new progress roadmap with a cyber workforce consisting of 225,000 people with this plan. He stated that employing the most talented workforce, developing a corporate culture, and implementing reforms in operations are necessary to strengthen cybersecurity (Oktay, 2023).

China prioritizes preventing damage to the country's critical infrastructure in cyber actions, preventing any virtual files from harming social order, economic development processes, and individual property rights, and preventing activities that would harm military capacity (Swaine, 2013). According to Gierow (2015), China aims to produce its information technology to avoid the hegemony of leading countries in the sector and to maintain national sovereignty in this field as well (Gierow, 2015). Similarly, The State Council Information Office (SCIO) of China published a white paper titled "Building a Community with a Shared Future in Cyberspace" on November 7, 2022 (SCIO 2022). The report emphasizes the necessity of cooperation in cyberspace, the fact that the world has become a global village thanks to the internet, the increasing interconnectedness of international communities, and the

need to use the internet for the betterment and positive direction of humanity. It also highlights that as of June 2022, there are 1.05 billion internet users, and it hosts the world's largest 5G network. The same report also emphasizes China's active cooperation in cyberspace security, reform, and development of global cyberspace governance, and providing internet services to underdeveloped or developing countries.

Another battleground between the USA and China is social media. Both countries have entered fierce competition in this field to establish superiority over each other. For example, a tweet by the Chinese Embassy in the United States praising China's practice of restricting Uighur Turks from having children was removed from Twitter (Euronews, 2021). Especially during the COVID-19 pandemic, President Trump tweeted many of his accusatory words toward China. In these tweets, he touched on many issues such as the virus spreading from China and the need for compensation (Çavuş & Öztürk, 2021). And a tweet from the White House regarding vaccine allocation included the Taiwanese flag, which China considers its territory. In a statement from the White House, it was apologized for as an "honest mistake" (Moore, 2021). In addition, in 2020, US Secretary of State Mike Pompeo stated that the USA is "certainly looking at banning Chinese social media apps, including TikTok". The reason given for this decision was the security vulnerabilities caused by Chinese access to the personal information of American users (Singh &Kalia, 2020). However, China competes with US applications such as Google, WhatsApp, and Twitter (presently X) with its social media applications WeChat, Baidu, and TikTok. TikTok, a Chinese-origin short video-sharing application that wants to be more effective in this battleground, aims to increase its user base by introducing a text-sharing feature (Holpuch, 2023). Additionally, social media applications such as Facebook and Twitter, which are banned in China, have been opened for use by Chinese diplomats. With this change, it was stated that better communication with people outside the country will provide the opportunity to better express China and its policies on the international stage as a part of public diplomacy (University of Oxford, 2021).

Besides the virtual initiative, there has been a cold war-like conflict between the two countries. For example, the Chinese navy maneuvered the guided missile frigates Yulin and Hohnot, accompanied by a destroyer, near the islets it claims. Even before this maneuver was completed, the United States for the first time simultaneously conducted a maneuver with the USS Ronald Reagan and the USS Nimitz in the South China Sea, simulating a prolonged attack on the targets of an imaginary enemy (Yıldızoğlu, 2020).

3.2. The Gezi Park protests in Turkey

The Gezi Park protests emerged as a civil movement in response to the Justice and Development Party (AK Party) government's project to transform Taksim Square and Gezi Park in May 2023. It brought together various groups and individuals from different segments of society with different perspectives. The resistance, which originated as a reaction to the government's attempts to replace urban transformation and republican monuments with symbolic structures reflecting Ottoman-era architecture, gradually grew and transformed into a mass action (Akcan, 2015). During the Gezi Park protests, left-wing parties, unions and organizations, feminist groups, LGBT+ groups, environmentalists, and football club supporters participated with their emblems and banners. The Gezi protests serve as an important example of diverse groups coming together on a common ground to resist state power (Gambetti, 2014). During the Gezi Park protests, various groups including left-wing parties, unions and organizations, feminist groups, LGBT+ groups, environmentalists, and football club supporters actively participated, displaying their emblems and banners. The Gezi protests are significant as they demonstrate how diverse segments of society can unite on a common platform to resist the power of the state (Gambetti, 2014).

The Gezi Park resistance was not limited to the protests held in Taksim, Istanbul, but spread throughout the city and eventually across Turkey with the help of social media platforms using hashtags such as #DirenGezi (#OccupyGezi). The movement also gained international support. Digital activism was employed to try to prevent police intervention and violence during the protests. Additionally, due to the divisive and derogatory statements made by then-Prime Minister Recep Tayyip Erdoğan and the increase in police violence, the hacktivist group Anonymous hacked the Prime Ministry's website (Baban & Güzel, 2015). These examples demonstrate how a local protest can gain global significance and empower non-state actors through digital activism and hacktivism. Mainstream mass media, however, either did not cover the Gezi movement or attempted to suppress it due to government pressure. Media outlets under the supervision of the Turkish Radio and Television Supreme Board (RTUK) that reported on the Gezi protests were either shut down or faced penalties such as blackouts or warnings (Vatikiotis & Yörük, 2016).

Gezi Park protests were characterized by a conflict between state and non-state actors. Various civilian groups from different segments of society engaged in a struggle against the regular police forces of the state. The government used police violence as a means of hard power and attempted to suppress the coverage of events by exerting pressure on the media. In response, civilian groups occupied public spaces, organized mass marches and sit-ins, employed discursive practices, and conducted demonstrations accompanied by wall writings, posters, slogans, music, and chants. They effectively utilized social media to garner support and spread the protests worldwide. The use of social media and the internet played a significant role in breaking the disproportionate power dynamics between the parties involved.

During the approximately three-week-long protests, one police officer and eight civilians lost their lives, nearly 10,000 people were injured, and an investigation led to the preparation of indictments against 17 individuals. As a result, the government was unable to realize its project concerning Gezi Park (BBC, 2023).

3.3. Theodore John Kaczynski (aka Unabomber)

Theodore John Kaczynski, also known as the Unabomber, began his studies at Harvard University at the age of 16 and had an IQ score of 167. He obtained his bachelor’s degree from Harvard, a master's and a doctoral degree in mathematics from the University of Michigan, and worked as an assistant professor at the University of California for 2 years (Kacynski, 2009). During his university years, Kaczynski developed an interest in natural and primitive living. When one of his favorite natural habitats was destroyed to build a road, he decided to carry out bomb attacks against technology and the industrial system. After leaving his job at the university, he built a secluded cabin in Montana where he lived for 24 years, away from the amenities provided by technology (electricity, water, heating, etc.). He carried out his bombing campaign for 18 years before being captured in 1996 and sentenced to life in prison without parole. He was found dead in his prison cell at the age of 81 (Warren, 2017; Murphy, 2023).

The turning point in Kaczynski's story was the publication of his 35,000-word manifesto, in which he explained his views on modern life and the reasons that led him to take action. The manifesto, published in The Washington Post and The New York Times, was made accessible to thousands of people. Kaczynski's brother, David, recognized the author's writing style, leading to a raid on his cabin where the typewriter used to write the manifesto was found (FBI 2023).

During his approximately 17-year-long campaign from 1978 to 1995, Kaczynski sent homemade bomb packages to airports and technology-related departments at universities, resulting in the deaths of 3 people and injuries to 23 others (Ray, 2023b). Kaczynski initially

adopted a strategy of using violent force against the industrial system and sent bomb packages to units representing technology. He manufactured and tested his bombs in his secluded cabin and managed to avoid capture for a long time. His communication with the FBI and the publication of his manifesto in newspapers signaled his adoption of soft power. The manifesto allowed him to communicate with the public and convey his purpose and the reasons behind his actions. Over time, Kaczynski became popularly known as the "Unabomber," and there are two documentaries about him available on the popular video-sharing platform Netflix (see Imbd, 2017; Netflix, 2017; Netflix, 2018). His manifesto was published as a book and translated into various languages (see Kacynski, 2023). While in prison, he responded to the letters he received and continued to advocate for his case. Although Kaczynski aimed to dismantle the industrial system through technology, the spread of his mission was also facilitated by technology. Today, anyone curious about him can easily access information about him online, and academics conduct studies examining his views and actions. This suggests that his war continues in some form. Therefore, it is appropriate to consider his actions within the context of a "smart war."

3.4. Anonymous hacker group

Anonymous, an activist hacker group with unidentified members worldwide, operates with an anarchist perspective and lacks a formal structure. The group aims to make the world a better place and has been involved in impactful actions such as targeting the Scientology cult, AlQaeda, Islamic State (ISIS), PayPal, the United Nations, and Russian attacks (Cybervie, 2023). The Anonymous group defines themselves with the following words on their website, anonymoushack.net:

> …it’s more of a loose collective, a digital movement made up of individuals who come together for various reasons. This collective lacks a formal hierarchy or centralized leadership, making it difficult to pin down a definitive description. Their symbol, the Guy Fawkes mask, borrowed from the movie “V for Vendetta,” has become a recognizable emblem of their movement. (Anonymous Hackers 2023)

In February 2022, following Russia's invasion of Ukraine, the Anonymous Twitter account with 7.9 million followers declared war on Russia and subsequently launched attacks on Russian websites. These attacks rendered government institutions, state-controlled news sources, and companies’ websites inoperable and resulted in data leaks (Huddleston, Jr., 2022). During that time, over 1,500 Russian websites were targeted. Among the hacked sites were RT, the Ministry of Defense, Gazprom, the Federal Space Agency (ROSCOSMOS), and TV channels (MNSBC, 2022). In the cyber-attacks carried out by Anonymous, a significant number of files in the targeted websites' databases were deleted (approximately 92%), and pro-Ukraine messages were left in their place (for example, folders with the title "Putin stop war" were placed instead of the deleted files) (Fowler, 2023). According to Jeremiah Fowler, a cybersecurity expert and the founder of Security Discovery, these attacks exposed Russia's vulnerability in the field of cybersecurity and shattered the Iron Curtain image (Pitrelli, 2022).

Anonymous's cyber-attacks on organized forces, states, and groups with an image of "strong oppressors" can be considered part of the "hard power" strategy. The group's Guy Fawkes mask, social media accounts, articles shared on its website, and hacking training are soft power strategies. Anonymous is a group of unidentified individuals with an uncertain hierarchical structure and center of control and has public support. Anonymous used "smartly” its soft and hard power strategies to intervene in the Ukrainian-Russian war and succeeded in damaging Russia's strong image. In this context, Anonymous's activities are evaluated within the framework of smart warfare.

3.5. Edward Snowden

Edward Snowden, the actor of the most important CIA disclosure of "Wikileaks", which was closely followed by the world agenda for a while, was born on June 21, 1983, in North Carolina. In 2009, he left the CIA and started working for the National Security Agency. There, being suspected of trying to access top-secret files about surveillance activities of the NSA, he left and moved to Dell, an NSA subcontractor, as a private contractor, and then to Booz Allen (Biography, 2019) In 2013, he made public various information about the secret information gathering programs conducted by the NSA (Ray, 2023a). There have been many espionage and intelligence activities throughout history, but unlike these standard espionage activities, Snowden was the first agent to reveal the inter-state intelligence struggle via cyber espionage (Sezgin, 2014). Observing the change in Obama's intelligence activities, Snowden decided to share the information with the public when he saw that there was no change. While working in the Hawaii office of Booz Allen, he began leaking information about US intelligence methods to The Guardian reporter Glenn Greenwald. On May 1, 2013, Snowden left his home in Hawaii and went to Hong Kong (Tüysüzoğlu, 2013). Speaking to The Guardian newspaper in Hong Kong, Snowden revealed in the first interview that the personal information of Verizon, one of the biggest telecom giants of the US, was taken by the US authorities. This news was published in the June 5, 2013, issue of The Guardian. On June 6, it was revealed that the NSA was using a program called Prism, which provides direct access to the data of Google, Facebook, Apple, and other US companies. These companies denied this and stated that they gave limited access to the US government. He also stated in an interview with the South China Morning Post on June 12, 2013, that the NSA had been hacking into Chinese computers since 2009 (Sezgin, 2014). In response to this incident, the US government accused Snowden of theft of government property, unauthorized transmission of national defense information, and intentional transmission of classified communications intelligence information to an unauthorized person. The last two charges led to a public amnesty campaign on Snowden's behalf. More than a hundred thousand people signed a petition for Snowden's pardon by the end of June 2013 (Biography, 2019). After these developments, Snowden sought asylum in Russia. He stated that in 2013 he was offered asylum in Venezuela, Nicaragua, and Bolivia, but he preferred Russia. The US asked Russia to extradite Snowden, but Russia refused.

Snowden started a fight against the USA leaked top-secret information and then defected to Russia. The USA charged him with the Espionage Act, but he also received public support. He gave interviews to newspapers and played his own life in the documentary, Citizenfour directed by Laura Poitras (IMDb, 2014). The documentary won an Oscar for Best Documentary Feature at the 2015 Academy Awards (The Guardian, 2023). And in 2016 the movie Snowden was released directed by Oliver Stone (See; IMDb, 2016). The initial activities of Snowden can be considered as a hard strategy. Leaking top secret documents was a threat to the US Government to stop surveillance activities. He also used a soft strategy and connected to public opinion by revealing top-secret information. Documentary and film contributed to his positive image. Although the USA charged him with espionage, public opinion embraced his activities. He starred in the documentary of his own life and won an Oscar. Snowden used information and communication technologies to win the war he started a powerful state, the USA. Therefore, the Snowden case was considered an example of a smart war between an individual actor and a state.

Conclusions

Starting in the first half of the 20th century and triggered by exponential technological developments, the concept of smart war does not yet have an adequate theoretical definition. To clarify and explain the concept of smart war, a theoretical framework that explains the

concept in four basic dimensions has been developed. A new definition has been introduced to the literature based on the components of the antecedents, actors, technologies, and strategies. According to this definition, smart War is a type of war that involves state and non-state actors, triggered by developments in Information Technology, where components of information technology are used as weapons and aim to gain superiority over the enemy by following a smart war strategy.

This article aimed to provide a theoretical framework for the concept of smart warfare. The concept of smart warfare was developed based on information technology. The developed theoretical framework is analyzed through examples and the operability of the theory is evaluated. The results obtained show that the conflicts that occurred after the emergence of information technologies have common points, and that the definition of smart war can be made based on these commonalities. Future research can improve the theory by approaching the concept of smart war from different perspectives. Research can be conducted on different dimensions of smart warfare. For example, examples can be studied at the level of countries, non-state actors, and individuals. In terms of strategy, soft strategy and hard strategy applications and future research can contribute to the development of the theory.

References

Ackoff, R.(1989). From data to wisdom. *Journal of Applied Systems Analysis*,16(1), 3-9.

Akcan, E. (2015). The "Occupy" Turn in the global city paradigm: The architecture of AK Party's Istanbul and Gezi Movement." *Journal of the Ottoman and Turkish Studies Association 2*(2), 359–378.

Akçay, N. (2020, Aug 18). ABD-Çin mücadelesinin arka planı: Teknoloji savaşları. Retrieved May 15, 2023, from https://www.indyturk.com/node/228641/t%C3%BCrkiyeden-sesler/abd-%C3%A7inm%C3%BCcadelesinin-arka-plan%C4%B1-teknoloji-sava%C5%9Flar%C4%B1

Alibaba (2023, Apr 11). Alibaba cloud unveils new AI model to support enterprises' intelligence transformation. Retrieved May 15, 2023 fromhttps://www.alibabagroup.com/en-US/document1582482069362049024

Alvarez-Junco, M.(2022). "smart war? ." [LinkedIn Post]Retrieved May 15, 2023 from https://www.linkedin.com/posts/manuel-alvarez-junco-6b57201a_smart-war-activity-6904709108692566016-1TXI/

Andrews, C. (2012). Smart warfare. *Engineering & Technology*,7(6), 56-59.

Anonymous Hackers (2023). Is Anonymous a group of hackers? [Blog post]Retrieved Aug 15, 2023 from https://www.anonymoushackers.net/anonymous-news/is-anonymous-a-group-of-hackers/

Arkin, W. M. (1999). In praise of heavy bombs. *The Bulletin of the Atomic Scientists*, 55(4): 80.

Aytekin, E. (2022, Dec 26). Çin, 2022'de ABD'nin 'çip savaşının' etkilerini hissetti [Press Release] Retrieved May 15, 2023 from https://www.aa.com.tr/tr/dunya/cin-2022de-abdnin-cip-savasinin-etkilerinihissetti/2772866

Baban, E. & Güzel, E. (2015). Digital activism and social movements: How the World perceives the Gezi Movement. *Amity Journal of Media and Communication Studies 5*(1-2), 16-26.

BBC (2023, May 31). 10. yılında Gezi Parkı eylemleri: Gün gün neler yaşandı? [Press Release]. Retrieved Aug15, 2023 from https://www.bbc.com/turkce/articles/cv21rz7lykdo

Biography (2019). Edward Snowden. *Biography*. Retrieved Aug15, 2023 from https://www.biography.com/activists/edward-snowden

Blomquist, K. (2022). In Pursuit of (Soft) Power: Chinese artificial intelligence governance in an age of great power competition (Master's thesis). University of Oxford, Oxford.

Bourgeois, D.T., Smith, J.L., Wang, S. and Mortati, J. (2019). *Information Systems for Business and Beyond.* Open Text Books.

Chang, E. Y. (2023). LLM Debate on the Middle East Conflict: Is it resolvable? Technical report, Stanford: Stanford University Infolab. Retrieved Nov 15, 2023 from https://www.researchgate.net/publication/374556828_LLM_Debate_on_the_Middle_East_Conflict_Is_It_Resolvable

Cıvaoğlu, G. (2022, Jan 15). Yeşiladamlar [Press Release] Retrieved Aug 15, 2023 fromhttps://www.milliyet.com.tr/yazarlar/guneri-civaoglu/yesil-adamlar-6681391

Cybervie. (2023). The Anonymous Hacker's Grup [Blog post] Retrieved Nov 15, 2023 from https://www.cybervie.com/blog/theanonymous-hackers-group/

Çavuş, S. & Öztürk, M. (2021). Kovid-19'un ABD-Çin ilişkilerine etkisini Trump'ın Twitter'daki hakikat ötesi siyaseti üzerinden okumak. *Gümüşhane Üniversitesi Sosyal Bilimler Dergisi*,12(2), 389-403.

Daylight, E. G. (2015). Towards a historical notion of 'Turing-the father of computer science'. *History and Philosophy of Logic*, 36(3), 205-228.

DoD. (2023). DoD Cyber workforce strategy implementation plan 2023-2027. *Department of Defence Office of Republication and Security Review*. Retrieved October 17, 2023 from https://media.defense.gov/2023/Aug/03/2003274088/-1/-1/1/2023-2027-DOD-CYBER-WORKFORCE-STRATEGY-IMPLEMENTATION-PLAN.PDF

Euronews (2021, Jan 10). Twitter, Çin'in ABD Büyükelçiliği'nin Uygur kadınlarına yönelik paylaşımını kaldırdı [Press Release] Retrieved May 15, 2023 from https://tr.euronews.com/2021/01/10/twitter-cin-in-abd-buyukelciligi-nin-uygur-kadinlarina-yonelik-paylasimini-kaldirdi

Farris, K. (2000). Chinese views on information warfare. *Defense Intelligence Journal*,10(1), 38.

FBI (2023). The Unabomber. Retrieved Nov 15, 2023 from https://www.fbi.gov/history/famous-cases/unabomber

Fowler, J. (2023). Hacker group Anonymous and others targeting Russian data [blog post] Retrieved Jan 10, 2024 from https://www.websiteplanet.com/blog/cyberwarfare-ukraine-anonymous/

Gambetti, Z. (2014). Occupy Gezi as politics of the body. In Umut Özkırımlı (Ed.) *The Making of a Protest Movement in Turkey: #Occupygezi* (pp. 89-102). Palgrave-Pivot.

Gierow, H.J.J.(2015). Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses. *China Monitor,* (22), Retrieved Aug 15, 2023 from https://merics.org/sites/default/files/2020-05/150407_MERICS%20China%20Monitor%2022_en.pdf

Glaser, B. and Strauss A.L. (2017). *Grounded theory: the discovery of grounded theory*. New York, Routledge.

Goldstine, H H. & Goldstine, A.(1946). The electronic numerical integrator and computer (ENIAC). *Mathematical Tables and Other Aids to Computation*,2(15), 97-110.

Günyol, A.& Yılmaz, E. (2023, Aug 8). Çip çekişmesinde Çin'den yeni hamle. [Press Release] Retrieved Nov 15, 2023 from https://www.aa.com.tr/tr/dunya/cip-cekismesinde-cinden-yeni-hamle/2963421

History.com (2020). The space race. history.com. Retrieved Aug 15, 2023 from https://www.history.com/topics/cold-war/space-race

Hocaoğlu, M.F.&Genç, İ. (2019). Smart combat simulations in terms of industry 4.0. In M. Gunal (Ed.), *Simulation for industry 4.0* (pp. 247-273), Springer, Cham.

Hodge, C.C. (2000) Casual war: NATO's intervention in Kosovo. *Ethics & International Affairs 14*, 39-54.
Hoffman, F.G. (2009). Hybrid warfare and challenges. *JFQ*, 52, 34-48. Retrieved May 15, 2023 from https://apps.dtic.mil/sti/pdfs/ADA516871.pdf
Holpuch, A. (2023, Jul 25). TikTok introduces text-only posts [Press Release]. Retrieved Nov 15, 2023 from https://www.nytimes.com/2023/07/25/technology/tiktok-text-posts.html
Huddleston, Jr., T. (2022, Mar 25). 4chan trolling to launching cyberattacks on Russia [Press Release] Retrieved May 15, 2023 from https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html
IMDb (2014). Citizenfour. Retrieved May 15, 2023 from https://www.imdb.com/title/tt4044364/
IMDb (2016). Snowden. Retrieved May 15, 2023 from https://www.imdb.com/title/tt3774114/
IMDb (2017). Manhunt: Unabomber. Retrieved May 15, 2023 from https://www.imdb.com/video/vi2297083929/?playlistId=tt5618256&ref_=tt_ov_vi
Imran, L. B., Farhan, M., Latif, RMA. & Rafiq, A. (2018). Design of an IoT based warfare car robot using sensor network connectivity. ICFNDS'18: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. Amman, Jordan: Assoc Comp Machinery.
Josan, A. & Voicu, C.(2015). Hybrid wars in the age of asymmetric conflicts. *Review of the Air Force Academy 1*(28), 49-52.
Kacynski, T. J. (2023). *The Unabomber manifesto: industrial society and its future*. BoD-Books on Demand.
Kacynski, T.J. (2009). Letter to a Turkish anarchist. *The Anarchist Library*. Retrieved May 25, 2023 fromhttps://theanarchistlibrary.org/library/ted-kaczynski-letter-to-a-turkish-anarchist
Kemaloğlu, İ. (2016). 21. Yüzyılın başında Rusya Federasyonu. *Marmara Türkiyat Araştırmaları,*3(2): 1-14.
Kharpal, A. (2023, Jun 1). Alibaba begins rollout of its ChatGPT-style tech as China AI race heats up [Press Release]. Retrieved Nov 15, 2023 from https://www.cnbc.com/2023/06/01/alibaba-rolls-out-chatgpt-style-tech-as-china-ai-race-heats-up.html
Kiss, P.A. (2014). *Winning wars amongst the people: case studies in asymmetric conflict.* University of Nebraska Press
Konak, A. (2019). Kırım'ınilhakıilesonuçlananukraynakriziveekonomiketkileri.*Uluslararası AfroAvrasyaAraştırmalarıDergisi*,4(8), 80-93.
Laudon, Kenneth C, & Jane P Laudon (2022).*Management information systems: managing the digital firm (Global Edition)*. 17. Pearson Education Limited.
Lukasik, S.J. (2011). Why the Arpanet was built. *IEEE Annals of the History of Computing*,33(3), 4-21.
McCarthy, J, Minsky, ML., Rochester, N. and Shannon, C.E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence, August 31, 1955. *AI Magazine*,27(4), 12- 14.
MNSBC (2022). Hacker group Anonymous declares 'cyber war' on Putin's Russia [Video] Retrieved May 15, 2023 from https://www.youtube.com/watch?v=gkrDIjGP4_w
Moor, J. (2006). The Dartmouth College artificial intelligence conference: The next fifty years. *AI Magazine*,27(4), 87-91.
Moore, M. (2021, Jul 8). White House Brushes off Deleted Taiwan Tweet as an 'Honest Mistake' [Press Release].Retrieved May 15, 2023 from

https://nypost.com/2021/07/08/white-house-calls-deleted-taiwan-tweet-an-honest-mistake/
Murphy, M. (2023, Jun 10). Unabomber Ted Kaczynski found dead in US prison cell [Press release] Retrieved Nov 15, 2023 fromhttps://www.bbc.com/news/world-us-canada-65867291
National Science Foundation (2023). Chips and Science. National Science Foundation. Retrieved Dec 15, 2023 from https://new.nsf.gov/chips#what
Netflix (2017). Manhunt: Unabomber. Retrieved May 15, 2023 from https://www.netflix.com/tr/title/80176878
Netflix (2018). Unabomber - In his own words. Netflix. Retrieved May 15, 2023 from https://www.netflix.com/tr/title/81002216
Nye, J.S. (2009). Get smart: combining hard and soft power. *Foreign Affairs*,88(4), 160-163.
Normand, R. (2001). Sanctions against Iraq: Is it genocide? *Guild Prac*. 58, 27.
Nye, J.S. (2019). Soft power and public diplomacy revisited. *The Hague Journal of Diplomacy*,14, 7-20.
Nye, J.S. (2023). State smart power strategies. In *Soft power and great-power competition: China and globalisation* (pp.21-28). Singapore: Springer.
Oktay, M. (2023, Aug 4). Pentagon: Siber altyapımızı güçlendirecek yeni bir program başlattık. [Press Release]. Retrieved Nov 15, 2023, from https://www.aa.com.tr/tr/dunya/pentagon-siber-altyapimizi-guclendirecekyeni-bir-program-baslattik/2961001
OpenAI (2022, Nov 30). Introducing ChatGPT [Blog post]. Retrieved May 15, 2023 from https://openai.com/blog/chatgpt
Pathak, A.D., Saran, D., Mishra, S., Hitesh, M.,Bathula, S. & Sahu, K.K.(2021). Smart war on COVID-19 and global pandemics. In Chhabi Rani Panigrahi, BibudhenduPati, MamataRath, RajkumarBuyya (Eds.) C*omputational Modeling And Data Analysisin COVID-19 Research* (p.28), CRC Press.
Perry, D.G., Blumenthal, S.H.&Hinden, RM.(1988). The ARPANET and the DARPA Internet. *Library Hi Tech*, 6(2), 51-62.
Pitrelli, M. (2022, Jul 29). Hacktivist group Anonymous is using six top techniques to 'embarrass' Russia [Press Release]. Retrieved from May 15, 2023 from https://www.cnbc.com/2022/07/28/how-is-anonymous-attacking-russia-the-top-six-ways-ranked-.html
Preußger, P. (2023, Apr 3). Visions of a smart war? image and ethics of autonomous weapon systems [Blog post], Retrieved Aug 26, 2023 from Philipp Preußger // Visions of a Smart War? Image and Ethics of Autonomous Weapon Systems — SchauflerLab@TU Dresden — TU Dresden (tu-dresden.de)
Qi, H. (2021). Smart' warfare and China–U.S. stability: strengths, myths, and risks *China International Strategy Review*, (3), 278–299.
Ray, M. (2023a). Edward Snowden.Retrieved Dec 25, 2023 from https://www.britannica.com/biography/Edward-Snowden.
Ray, M. (2023b). Ted Kaczynski. Britannica Retrieved Dec 25, 2023 from https://www.britannica.com/biography/Ted-Kaczynski
Renz, B. (2016). Russia and 'Hybrid Warfare'. *Contemporary Politics*, 22(3), 283-300.
Robinson, A. (2014, Oct 18). The enduring enigma of Alan Turing. Retrieved Jul 18, 2023 from https://www.thelancet.com/action/showPdf?pii=S0140-6736%2814%2961854-7
Rosenberg, P. (2013, Sep 10). Obama's error: Getting beyond the 'smart war' syndrome. Retrieved Jun 27, 2023 from https://www.aljazeera.com/opinions/2013/9/10/obamas-error-getting-beyond-the-smart-war-syndrome

Rowe, J. C. (1991). The "Vietnam Effect" in the Persian Gulf War. *Cultural Critique Autumn*, (19), 121-139.

Sample, I. (2003). US Gambles on a 'smart' war - the military is relying on precision weapons to both win the war in Iraq and help prevent politically damning civilian casualties. But the technology is far from fail-safe. *New Scientist, 177*(2387), 6-7.

Schneider, G.P. (2017). *Electronic commerce*. Boston: Cengage Learning.

SCIO (2022). Jointly Build a community with a shared future in cyberspace—the State Council Information Office of the People's Republic of China. Retrieved May 15, 2023 from http://english.scio.gov.cn/node_8033411.html

Sezgin, F. (2014). Edward Snowden olayı'nın ABD-Rusya ilişkileri üzerindeki etkisi. *Uluslararası Yönetim ve Sosyal Araştırmalar Dergisi*,1*(*1): 24-31.

Simons, A. (2012, Apr 27). Soft war = Smart war? Think again. Retrieved May 15, 2023 from https://www.fpri.org/article/2012/04/soft-war-smart-war-think-again/

Singh, K., and Kalia, S. (2020, Jul 7). Pompeo says U.S. looking at banning Chinese social media apps, including TikTok [Press Release]Retrieved May 15, 2023 from https://www.reuters.com/article/us-usatiktok-china-pompeo-idUSKBN2480DF

Schmitt, M.N. (1999). The principle of discrimination in 21st-century warfare. *Yale Human Rights and Development Journal*,2(1), 143-182.

Swaine, M.D. (2013). Chinese Views on cybersecurity in foreign relations. *China Leadership Monitor*, no. 42. Retrieved May 15, 2023 from https://carnegieendowment.org/files/CLM42MS.pdf

The Guardian (2023, Feb 23). Edward Snowden documentary citizen four wins oscar. Retrieved May 15, 2023 fromhttps://www.theguardian.com/film/2015/feb/23/edward-snowden-documentary-citizenfour-wins-oscar

The White House (2023). National cybersecurity strategy. Washington. Retrieved May 15, 2023 from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Thornton, R. (2007). *Asymmetric warfare: threat and response in the twenty-first century*. Polity.

Turing, A.M. (1937). On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc.* 42(2), 230-265.

Turing, A.M. (1950). Computing machinery and intelligence. *Mind,* 59(236), 433-460.

Turing, A.M. (1937). On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc*,.42(2), 230-265.

Tüysüzoğlu, G. (2013, Jul 16). Post-modern bir casusluk hikayesinin kahramanı: Edward Snowden [Blog post]. Retrieved May 15, 2023 from https://www.tuicakademi.org/post-modern-bir-casusluk-hikayesinin-kahramani-edward-snowden/

Tzu, S. (1963). *The Art of War* (Translated by Samuel B Griffith). USA: Oxford University Press.

University of Oxford (2021, May 11). Fanatic fans or fake followers? Chinese diplomats and their social media networks. Retrieved May 15, 2023 from https://www.ox.ac.uk/news/2021-05-11-fanatic-fans-or-fake-followers-chinese-diplomats-and-their-social-media-networks

Vatikiotis, P.&Yörük, ZF. (2016). Gezi movement and the networked public sphere: A comparative analysis in global context. *Social Media + Society*, July-September, 1-12.

Warden, J. (2008). War modeling & simulation. Let's start at the end - a very good place to start. Venturist. Retrieved May 15, 2023 from https://apps.dtic.mil/sti/citations/ADA501007

Warren, D.C. (2017). Ted Kaczynski: evil or insane? *The Cupola.* Retrieved May 15, 2023 from https://cupola.gettysburg.edu/cgi/viewcontent.cgi?article=1650&context=student_scholarship

Weik, M.H. (1961). The ENIAC Story. *Ordnance*,45(244), 571-575.

Wither, J.K. (2016). Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal*,15*(*2), 73-87.

Wolfswinkel, JF, Furtmueller, E. & Wilderom, CPM. (2011). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*,22(1), 45-55.

Yan, G. (2020). The impact of artificial intelligence on hybrid warfare. *Small Wars & Insurgencies*, 31(4), 898-917.

Yeon-Bong, J. (2019). A Study on Implications of U. S. Army Revolution in Military Affairs(RMA) to ROK Army RMA. 군사연구, 147, 285-314. Retrieved May 15, 2023 from https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE09239789.

Yıldızoğlu, E. (2020, Jul 14). ABD ve Çin arasındaki 'yeni soğuk savaş' dünya için ne kadar büyük bir risk? Retrieved May 15, 2023 from https://www.bbc.com/turkce/haberler-dunya-53404403.

Zhu, Z. (2020, May 15). Interpreting China's 'wolf-warrior diplomacy'. Retrieved May 15, 2023 fromhttps://thediplomat.com/2020/05/interpreting-chinas-wolf-warrior-diplomacy/

View publication stats