CYBERSECURITY AND AI

Dumitru BUDACU
Alexandru Ioan Cuza University of Iași, Romania

THE IMPACT OF THE ARTIFICIAL INTELLIGENCE ON HYBRID CONFLICTS IN THE 21ST CENTURY

Abstract: *Hybrid conflict, from an artificial intelligence perspective, refers to complex and multifaceted conflict in which different methods of warfare are used in a coordinated manner to achieve strategic objectives. Artificial intelligence can play a significant role in both executing and defending against 21st century conflicts. Hybrid conflicts are characterized by the blending of conventional and unconventional tactics, often involving a combination of military force, cyber operations, economic coercion and information warfare. Some notable examples where elements of hybrid conflict have been observed are Russia – Ukraine Conflict (2014 – present), Syrian Civil War (2011 – present), Crimea Annexation (2014), Iranian Proxy wars and Cyber Operations, China's Strategy in the South China Sea, Baltic states and Russian Influence Operations. The role of artificial intelligence in countering Hybrid conflict is to detect and analyze threats, shape automated response systems, support strategic decisions, and build resilience.*

The impact of artificial intelligence on hybrid conflict in the 21st century is profound and multifaceted. While offering significant advantages in intelligence, cyber operations and decision-making, it also introduces new risks and ethical dilemmas. As artificial intelligence continues to evolve, its role in hybrid conflicts is likely to expand, becoming a key factor in future military and geopolitical strategies. To meet these challenges, it is essential that nations develop robust frameworks for responsible use of artificial intelligence in warfare, ensuring that its benefits are exploited while minimizing risks. It is certain that the ability of AI to quickly and accurately process and analyze large amounts of information, which can be exploited to either execute or counter these multifaced strategies, will be a major challenge for all of us in the years ahead.

Keywords: **Artificial intelligence; conflict; ethics; hybrid conflict; operations; tactics;**

Contact details of the authors: E-mail: budacu_dumitru@yahoo.com

Institutional affiliation of the authors: **Alexandru Ioan Cuza University of Iași, Romania**

Institutions address: Bulevardul Carol I, Nr.11, 700506, Iaşi, România, 0040/0232 20 1000, www.uaic.ro

Terminology clarifications

For our study we have used two concepts, namely artificial intelligence and conflict. In the following, we will briefly specify these two concepts.

Artificial intelligence. Emergence and evolution

Intelligence is the capacity of a being to learn, understand and use knowledge and skills and abilities to solve problems, adapt behavior to new situations, make decisions and create innovative solutions. This involves complex brain processes such as perception, reasoning, memory, creativity and the ability to make logical connections. According to different psychological theories, there are several types of intelligence: *logical-mathematical intelligence* (the ability to think logically, solve problems and work with mathematical concepts), *linguistic intelligence* (the ability to use language to communicate effectively, to write and to understand the subtleties of language), *spatial intelligence* (the ability to visualize objects and spaces and understand the relationships between them), *interpersonal intelligence* (the ability to understand and interact well with other people), *intrapersonal intelligence* (the ability to understand oneself, to recognize one's own emotions and to manage them), *naturalistic intelligence* (the ability to understand and interact effectively with the environment), and *kinesthetic intelligence* (the ability to use one's own body to express ideas and perform physical activities).

Moreover, in recent years the concept of artificial intelligence has become increasingly relevant. Artificial intelligence refers to the ability of computers and machines to mimic some of the functions of human intelligence, such as pattern recognition, natural language processing, decision making and even learning. The term artificial intelligence was first used in 1956 by the American computer scientist John McCarthy, who is considered one of the fathers of the field. McCarthy introduced the term at a conference held at Dartmouth College in Hanover, New Hampshire, to investigate the possibilities of creating machines capable of simulating human cognitive processes. While initially the term artificial intelligence was used to designate any effort to make machines "intelligent", i.e. capable of mimicking or simulating human cognitive functions, today artificial intelligence has become a general term for a vast field that includes *machine learning* (algorithms that learn from data and improve performance over time), *deep learning* (complex neural network models, used for tasks such as facial recognition or machine translation), *natural language processing* (understanding and generating human text and speech) and *general artificial intelligence* (a theoretical concept of an artificial intelligence capable of a wide range of human-like cognitive tasks).

The term artificial intelligence, originally used to describe attempts to create machines that can 'think' like humans, has since become synonymous with a broad field of science that is increasingly influencing many aspects of modern life, and certainly in the future our lives will certainly be influenced and changed by artificial intelligence. To this distinctive capacity our species owes its dominant position. If machine brains surpass human brains in general intelligence, then this new superintelligence could become extremely powerful, possibly beyond our control[1].

Deep learning is a form of machine learning that allows computers to learn from experience and understand the world in terms of a hierarchy of concepts. Because the computer accumulates knowledge from experience, there is no need for a human computer operator to formally specify all the knowledge the computer needs. Concept hierarchies allow the computer to learn complicated concepts by building them from simpler concepts; a graph of these hierarchies would have many layers of depth. This book covers a wide range of topics in deep learning[2]. Reinforcement learning, one of the most active areas of research in artificial intelligence, is a computational approach to learning in which an agent attempts to maximize the total amount of reward it receives when interacting with a complex and uncertain environment[3]. Deep learning has stimulated the whole field of machine learning[4]. Inevitably we can turn to a few questions when it comes to artificial intelligence, namely How smart are the best artificial intelligence programs really? How do they work? What can they do and when do they fail? How human-like do we expect them to become, and how quickly do we need to worry that they'll outperform us? Along the way, she introduces the dominant models of modern artificial intelligence and machine learning, describing cutting-edge artificial intelligence programs, their human inventors, and the historical lines of thought underlying recent achievements[5].

To conclude by saying that artificial intelligence powers Google's search engine, allows Facebook to target advertising, and allows Alexa and Siri to do their jobs. AI also underpins self-driving cars, predictive policing and autonomous weapons that can kill without human intervention. These and other applications of AI raise complex ethical issues that are the subject of ongoing debate[6].

The concept of conflict. Evolution and diversity

The general term conflict can be understood as a situation in which two or more parties (individuals, groups, organizations or even countries) have interests, needs, values or goals that are opposed or incompatible and lead to tensions, disagreements or confrontations. Conflicts can arise in different contexts (in personal

[1] Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press, 2016, p. 57

[2] Ian Goodfellow, Yoshua Bengio Courville, *Deep Learning*, The MIT Press, 2016, p. 33

[3] Andrew C. Barto, Richard S. Sutton, *Reinforcement Learning: An Introduction*, Bradford Books, 2018, p. 19

[4] Aurélien Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, And TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, O'Reilly Media, 2019, p. 47

[5] Melanie Mitchell, *Artificial Intelligence: A Guide for Thinking Human*. Farrar, Straus and Giroux, 2019, p. 98

[6] Mark Coeckelbergh, *AI Ethics*, The MIT Press, 2020, p. 44

relationships, at work, in society or internationally). Conflicts are of different types *interpersonal conflict* (between individuals because of personality differences, opinions or disagreements), *intra-personal conflict* (occurs within a person, when they are faced with difficult choices, internal contradictions or conflicts between their own values and desires), *group conflict* (occurs between groups/teams with different goals, values or interests), *organizational conflict* (occurs within an organization and may be related to differences in business priorities, management styles or available resources), and *international conflict* (occurs between nations/large groups of people and may include political, economic or military conflicts).

The causes of conflict can be: *different interests* (when two parties want opposing things), *differences in values* (when personal, cultural or religious values clash), *limited resources* (competition for scarce resources can lead to conflict), *poor communication* (lack of clear communication or misunderstandings can lead to tensions), *different perceptions* (how parties interpret a situation can create conflict, even if intentions are good). Resolving a conflict usually involves identifying the causes and finding a compromise. Settlement methods are diverse and can include *negotiation* (direct discussions to reach a solution that satisfies both parties), *mediation* (a neutral third party helps the parties find a solution), *arbitration* (an external person or conflict makes a binding decision for both parties), *dialog* and *active listening* (understanding each party's perspectives and needs to reach a common solution). Conflicts are a natural part of human interaction, and the way they are managed can either lead to peaceful resolution or escalation.

A *military conflict* is a violent confrontation between two or more parties, usually states or organized armed groups, in which armed forces are used to gain control over resources, territory or to impose their political will. Military conflicts range from small, small-scale confrontations to large-scale wars involving land, air and naval forces. The most common types of military conflicts are: *war* (extreme form of military conflict, with large-scale fighting between nations or coalitions of nations), *civil war* (conflict between groups or factions within the same country, usually over political power or independence), *asymmetric conflict* (occurs when a state or conventional army fights against a smaller force, such as insurgent or terrorist groups, using guerrilla tactics), *military intervention* (involves sending troops into another country to support or overthrow a government without a declaration of war), *limited military conflict* (a conflict between two or more countries that avoids full escalation of war, usually restricted to certain borders or regions).

What is most painful after a military conflict are its consequences. The consequences of a military conflict are: *loss of life* (a large number of military personnel are killed or wounded, as well as inevitably the collateral victims who are civilians, namely women, children and the elderly), *destruction of infrastructure* (military confrontations leave behind destroyed cities, roads and other structures), *humanitarian crises* (conflicts lead to refugees famine, lack of clean drinking water and other hardships for affected populations), *economic impact* (resources are squandered, trade is affected, and reconstruction costs are huge), *political* and *social instability* (wars destabilize affected regions, often leaving room for post-conflict chaos and violence). Inevitably any conflict and military conflicts can be resolved. The resolution of military conflicts involves *peace negotiations* (the two sides meet to discuss the terms of cessation of hostilities), *armistice agreements* (the two sides agree to temporarily or permanently cease hostilities), *international mediation* (international organizations such as the UN intervene to facilitate peace talks), *peacekeeping intervention* (peacekeeping troops are sent in to protect civilians and prevent the conflict from restarting). *Military conflicts* are among the most serious forms of conflict, with complex and long-lasting effects on societies and economies worldwide.

A *hybrid conflict* is a form of modern conflict that combines conventional (classical military) tactics with unconventional tactics (such as disinformation, cyber-attacks and subversive actions) to destabilize or influence an adversary without initiating an open military confrontation. In this type of conflict, the aggressor combines a variety of methods - *military*, *economic*, *political* and *informational* - to weaken a state or organization without attracting the international attention and retaliation that would be involved in a traditional war.

When referring to *the military methods* used in hybrid warfare, it should be kept in mind that hybrid warfare is a complex strategy in which conventional and unconventional tactics are used to destabilize, intimidate and undermine a target without directly engaging conventional forces. In this type of conflict, *military methods* are interwoven with *non-military actions* (such as information manipulation, cyber-attacks and political subversion) to gain strategic advantage. The main military methods used in hybrid warfare are: the use of special troops and clandestine forces, psychological operations and propaganda, propaganda and media manipulation, cyber-attacks, cyber warfare, information warfare, unconventional and asymmetric weapon systems, instigation of protest movements and riots, support of local actors or military groups, exploitation of ethnic and religious conflicts, economic mobilization and financial pressures, and the creation of “grey zones” and strategic ambiguity. The military methods of hybrid warfare are complemented by a wide range of unconventional and asymmetric techniques, which allow the attacking state to weaken the target without a conventional invasion. These tactics undermine the stability and responsiveness of the targeted country and create strategic ambiguity that makes international responses difficult.

The economic methods used in hybrid warfare are tactics of influence and economic pressure designed to weaken the target state, cause financial instability and reduce its ability to respond to other forms of aggression. These economic methods are often subtle and difficult to attribute to an attacking state, helping to maintain a “gray zone” in which responsibility is difficult to determine. Some of the main economic methods most often used in hybrid warfare are: economic sanctions and embargoes, currency and financial market manipulation, cyber-attacks on the financial system, corruption and subsidization of local economic groups, control over energy resources and supply, strategic investigations and the purchase of critical assets, economic sabotage and price manipulation, support for corruption and the underground economy, undermining confidence in financial institutions, creating economic dependence through credit and loans, and cornering the economic media market. These economic methods of hybrid warfare are part of a broader strategy of destabilization and influence, in which the attacking state attempts to weaken the economy without resorting to direct military confrontation. Tactics such as economic sanctions, manipulation of markets, support for the underground economy and strategic investment allow the aggressor to exert pressure on governments and influence the target country's economic and political decisions. In this way, economic warfare becomes a central component of hybrid warfare, helping to gain strategic advantage without escalating the conflict militarily.

The political methods of hybrid warfare are tactics designed to weaken the political stability, social cohesion and credibility of target governments without the use of direct military force. These tactics involve manipulating information, influencing political decisions and undermining public confidence in democratic institutions. These are just some of the political methods used in hybrid warfare: Undermining trust in state institutions, interfering in electoral processes, widespread propaganda and disinformation, supporting protest movements and the opposition, influencing government policies through agents of influence, creating and sustaining ethnic and religious conflicts, launching campaigns to delegitimize political leaders, promoting separatism and regional autonomy, influencing through cultural and ideological tools, using international organizations and diplomacy for pressure, co-opting and corrupting local media, undermining legislation and the rule of law. The political methods of hybrid warfare are designed to weaken the target state through subtle and indirect actions. Tactics such as disinformation, election meddling, support for separatist movements and instigation of ethnic conflicts contribute to political destabilization and division of society. These actions have a major impact on public confidence in the government and state institutions, making them vulnerable to further aggression and reducing national resilience.

The information methods in hybrid warfare are tactics by which the aggressor state manipulates information to influence public opinion, create confusion, undermine trust in government and weaken social cohesion. These methods use a variety of channels, from the media and social networks to cyber-attacks, and are essential in hybrid warfare because they allow the attacking state to exert indirect control over the perceptions and actions of the target state. The main information methods used in hybrid warfare are: disinformation (fake news), propaganda, psychological warfare, creation and distribution of conspiracy theories, manipulation of social networks, cyber-attacks on media and communication institutions, co-opting and influencing local media, intervention in external information flows (geo-blocking and geolocation), spying and data collection for manipulation, distortion or taking real information out of context, creation of “alternative sources” and fake news sites, flooding and manipulation of images and video content. Information methods in hybrid warfare are essential to destabilize the target state without resorting to direct violence. Through tactics of disinformation, propaganda and cyber-attacks, the attacking state can influence public perceptions, weakening trust in government and fragmenting social cohesion. These methods are difficult to counter, as they work subtly and blend into the daily lives of the target population, thus contributing to the aggressor's goals of an undeclared conflict strategy. Hybrid warfare is increasingly relevant today, with several high-profile examples demonstrating its use by state and non-state actors. Here are some of the most notable examples:

Russia's invasion of Ukraine (2022 - present)

Russia's large-scale invasion of Ukraine in 2023 exemplifies hybrid warfare, combining traditional military force with irregular tactics such as the use of mercenaries from groups like the Wagner Group. Russia has launched numerous cyberattacks against Ukraine, targeting critical infrastructure, government networks, and communications systems to disrupt Ukraine's defenses and governance. Disinformation campaigns have been used to manipulate domestic and international perceptions of the conflict, including spreading false reports about the reasons for the invasion, the nature of the conflict and the legitimacy of the Ukrainian leadership. Russia has used electricity supplies as leverage against European countries supporting Ukraine, reducing or cutting off gas supplies to create economic and political instability. The Russian invasion of Ukraine has been a significant and ongoing event, generating a substantial body of literature that examines the conflict from various angles, including military strategy, geopolitical implications and humanitarian impact.

When it comes to the conflict between Russia and Ukraine, it is certain that Russia's rapid rise to power over the past few years coupled with a stunning lack of international diplomacy on the part of its president, combined with the rapidly changing geopolitics of Europe, has led to the West being on a possible path to nuclear war, as is becoming increasingly clear in the Russia versus Ukraine conflict[1]. Today, Russia, the successor to the Soviet Union, has put Ukraine's independence back in its sights[2]. Ukraine is currently embroiled in a tense struggle with Russia to preserve its territorial integrity and political independence, but today's conflict is just the latest in a long history of struggles over Ukraine's territory and its existence as a sovereign nation[3]. New game-changing technologies, disappearing rules of the game, and distorted perceptions on both sides combine to lock Washington and Moscow into an escalating spiral they don't recognize. All the pieces are in place for a World War I-type tragedy that could be triggered by a small and unpredictable event. The Russia Trap shows that anticipating this danger is the most important step in preventing it[4]. One thing is certain and that is that neither side has been able to bring this conflict to a definitive conclusion[5]. The seeds of Russia's war against Ukraine and the West were sown more than a decade before. Ukraine in all its splendor: vast, defiant, resilient and full of wonder[6].

China's activities in the South China Sea

China uses a combination of its navy, coast guard and maritime police to assert its territorial claims in the South China Sea, including building artificial islands and militarizing them, as well as deploying fishing fleets to exercise control over disputed areas. China engages in “legal warfare” by using ambiguous interpretations of international law, particularly the United Nations Convention on the Law of the Sea (UNCLOS) to justify its actions. China also uses economic coercion such as trade restrictions against countries that challenge its claims. China uses state media and social media to promote its “narrative” on the South China Sea, attempting to legitimize its actions and discredit the opposing claims of other nations such as Vietnam and the Philippines.

China's rise on the world's oceans is attracting particular attention and could ultimately reshape the global balance of power during the 21st century[7]. The topic of whether and how to integrate a stronger China into a global maritime security partnership has not been adequately explored. But for practitioners to structure cooperation effectively, they warn, Washington and Beijing need to create sufficient political and institutional space. China's maritime power dates back thousands of years. China has one of the oldest naval traditions in the world. However, China has historically been a mainland state with a large land force and only a coastal navy with limited blue-water capability. The rise of modern China raises considerable regional and security issues, in addition to the economic and political competition for a rightful place in the power politics of the South Asian region, and therefore requires critical analysis. It is necessary to focus future strategies to meet

[1] Richard Shirreff, *War with Russia: An Urgent Warning from Senior Military Command*, Quercus, 2016, p. 47

[2] Anne Applebaum, *Red Famine: Stalin's War on Ukraine*, Doubleday, 2017, p. 11

[3] Serhii Plokhy, *The Gates of Europe: A History of Ukraine*, Basic Books, 2017, p. 19

[4] George Beebe, *The Russia Trap: How Our Shadow War with Russia Could Spiral into Catastrophe*, Thomas Dunne, 2019, p. 71

[5] Lawrence Freedman, *Ukraine and the Art of Strategy*, Oxford University Press, 2019, p. 88

[6] Christopher Miller, *The War Came to Us: Life and Death in Ukraine*, Bloomsbury Continuum, 2023, p. 54

[7] Andrew S. Erickson, Lyle J. Goldstein, Nan Li, *China, the United States, and 21st-Century Sea Power: Defining a maritime Security Partnership*, Naval Institute Press, 2010, p. 22

these challenges, both in the medium and long term[1]. The rise of China has upset the global balance of power. For decades, tensions have simmered in the region, but now the threat of direct superpower confrontation is becoming increasingly likely. Whoever controls these waters controls access between Europe, the Middle East, South Asia and the Pacific[2]. Over the past decade, the center of world power has quietly shifted from Europe to Asia. With oil reserves of several billion barrels, an estimated nine hundred trillion cubic meters of natural gas, and competing territorial claims dating back centuries, the South China Sea in particular is a boiling pot of potential conflict. The buildup of military forces in the area where the Western Pacific meets the unreported Indian Ocean means that this is likely to be a fulcrum for global war and peace for the foreseeable future. To understand the future of conflict in East Asia, we need to understand the goals and motivations of its leaders and people, at a time when every day's news seems to contain a new story, big or small, that is directly related to the conflicts in the South China Sea[3]. Great Powers, Great Strategies offers the analysis of a dozen experts on "global" approaches to the South China Sea dispute. By exploring the international dimensions of this regional hotspot, it is worth examining how the military, diplomatic and economic strategies of major global actors have contributed to solutions and exacerbated the potential for conflict[4].

Iran's regional influence operations

Iran supports various proxy groups in the Middle East, such as Hezbollah in Lebanon, the Houthis in Yemen and Shiite militias in Iraq and Syria. These groups conduct military operations and terrorist activities that analyze Iranian interests without Iran's direct involvement. Iran has been linked to cyber-attacks targeting critical infrastructure and government institutions in rival countries, including Saudi Arabia and Israel. Iran also uses cultural diplomacy, media and religious ties to influence political outcomes in neighboring countries. Worth analyzing is how the struggles between Shiites and Sunnis in the Middle East will affect the future of the region, offering insight into the brutal and long-running power struggles between Iran and Saudi Arabia for political and spiritual leadership of the Muslim world[5].

The United States and Iran have been engaged in an unrecognized secret war since the 1970s. This conflict has frustrated several US presidents, divided administrations and repeatedly threatened to bring the two nations to the brink of open war. From the Iranian Revolution to the secret negotiations between Iran and the United States after 9/11, from Iran's nuclear program to Qasem Soleimani's covert and lethal role, a vital new depth to our understanding of the "Iranian problem" and what the future may bring to this tense relationship represents one of the most significant challenges[6].

In recent years, significant attention has focused on the Islamic Republic of Iran's nuclear ambitions and the threat they pose to the United States and the West. Much less understood, however, has been the phenomenon of Iran's regional advance into America's own hemisphere, an intrusion that has both foreign policy and national security implications for the United States and its allies[7].

Another important challenge is to analyze how the Arab world got to this point, what is happening now, what the ramifications will be, how it will affect Israel, and what immediate actions need to be taken, including how Western leaders should respond. Consider all the major power players in the Middle East, the underlying issues, the Arab Spring, the fall of the Muslim Brotherhood, the rise of ISIS, the epic animosity between Sunni and Shia, the essence of the Syrian war, the role of the caliphate and jihad, and the impending nuclear arms race[8]. We are obligated to get to know these people - what the regime means to them and their

[1] Sandeep Dewan, *China's Maritime Ambitions and the PLA Navy*, Vij Books India, 2013, p. 17

[2] Bill Hayton, *The South China Sea: The Struggle for Power in Asia*, Yale University Press, 2014, p. 81

[3] Robert D. Kaplan, *Asia's Cauldron: The South China and the End of a Stable Pacific*, Random House Trade Papperbacks, 2015, p. 73

[4] Andreas Corr, *Great Powers, Grand Strategies: The New Game in the South China Sea*, Naval Institute Press, 2018, p. 54

[5] Vali Nasr, *The Shia Revival: How Conflicts within Islam Will Shape the Future*, W. W. Norton & Co Inc, 2007, p. 17

[6] David Crist, *The Twilight War: The Secret History of America's Thirty-Year Conflict with Iran*, Penguin Publishing Group, 2013, p. 77

[7] Ilan Berman, Joseph M. Humire, *Iran's Strategic Penetration of Latin America*, Lexington Books, 2016, p. 27

[8] Avi Melamed, *Inside the Middle East: Making Sense of the Most Dangerous and Complicated Region on Earth*, Skyhorse, 2016, p. 91

anxieties about the future of their revolutionary project, of what it means to be pro-regime in the Islamic Republic, challenging everything we think we know about Iran and revolution[1].

North Korea's cyber operations

North Korea has increasingly relied on cyberattacks as a means of hybrid warfare, targeting financial institutions, cryptocurrency exchanges and critical infrastructure around the world. I would mention among notable attacks only the Sony Pictures hack (2014) and the WannaCry ransomware attack (2017). Through cyber operations, North Korea is trying to evade international sanctions and finance its regime, so it has stolen billions of dollars through cyber heists, especially from cryptocurrency exchanges. North Korea uses cyber capabilities to spread propaganda and disinformation to influence perceptions and destabilize adversaries, both domestically and internationally. Identity Wars is a wide-ranging look at how anonymity influences politics, activism, religion and art. A firm defense of anonymity and exploration of certain tools and organizations, especially its evolution with the ubiquity of the internet is of utmost importance. Examining online identities, both fake and real, is essential reading for the age of social networks[2]. Cybersecurity always in the era of cyber conflict has played a significant role for all state actors, including North Korea[3].

Turkey's use of hybrid tactics in Syria and Libya

In Syria, Turkey supported various rebel groups against the Assad regime and Kurdish forces. In Libya, Turkey provided military and logistical support to the Government of National Accord (GNA) against the Libyan National Army (LNA). Turkey effectively used drones in these conflicts, providing air support to its close allies, carrying out strikes on targets of opposition forces. Turkey has used the media and social media to shape accounts of its involvement in these conflicts, presenting its actions as part of a broader strategy to promote regional stability and combat terrorism. Turkey's use of hybrid tactics in Syria and Libya is a complex and multifaceted topic, covering aspects of military strategy, political maneuvering, and influence operations. Turkey holds a unique position between East and West and, with the end of the Cold War, has the potential for influence. Freedom from the Russian threat allows it to examine its ties with the West, and political changes and shifts in power in the region give it the opportunity to forge new relationships with its neighbors in the Near and Middle East[4]. Of particular importance is the exploration of how Turkey's contested national identity has affected its foreign policy from the end of the Ottoman era to the present. Identity matters for foreign policy decisions, but it separates itself from etatist approaches by bringing the issue of identity into domestic politics[5]. Hybrid warfare has been an integral part of the historical landscape throughout the ages, but recently analysts have incorrectly labeled these conflicts as unique. Throughout history, great powers have faced adversaries that have used a combination of regular and irregular forces to nullify the advantage of the great power's superior conventional military force. Hybrid wars are labor-intensive and long-term affairs. Hybrid wars are also the most likely conflicts of the 21st century, as competitors use hybrid forces to deplete military capabilities in protracted campaigns of exhaustion[6].

The effects of the Arab Spring on Turkish foreign policy are worth investigating. The demands for democracy that began in Tunisia spread rapidly across the Arab Middle East and North Africa. The focus and dynamics of the Arab Spring varied according to the countries in which it took place. As a counterpoint to the status quo in the Middle East, the Arab Spring stimulated much debate, leading to the emergence of new regional actors[7]. It is also worth examining contemporary political relations between Turkey and the Middle East. In the light of the 2011 Arab uprisings, the Syrian crisis, the escalation of regional terrorism and the attempted military coup in Turkey, the dramatic fluctuations in Turkey's foreign policy towards the major Middle Eastern countries of Iran, Saudi Arabia, Egypt, Syria and Iraq are also worth analyzing, as well as the analysis of Turkey's deepening involvement in regional affairs in the Middle East, also addressing issues such

[1] Narges Bajoghli, *Iran Reframed: Anxieties of Power in the Islamic Republic*, Stanford University Press, 2019, p. 84

[2] Cole Stryker, *Hacking the Future: Privacy, Identity, and Anonymity on the Web*, Abrams Press, 2012, p. 77

[3] Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, Simon & Schuster, 2017, p. 61

[4] Barkey, Henry, J., *Reluctant Neighbor: Turkey's Role in the Middle East*, United States Institute of Peace, 1997, p. 77

[5] Hasan Kösebalaban, *Turkish Foreign Policy: Islam, Nationalism, and Globalization (Middle East Today)*, Palgrave Macmillan, 2011, p. 62

[6] Williamson Murray, Peter R. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, 2012, p. 15

[7] Ýdris Demir, *Turkey's Foreign Policy Towards the Middle East: Under the Shadow of the Arab*, Cambridge Scholars Publishing, 2016, p. 33

as terrorism, social and political movements and struggles for minority rights. While these issues have traditionally been seen as domestic matters, this book emphasizes their increasingly regional dimension and the implications for the foreign affairs of Turkey and the countries of the Middle East[1].

The understanding of contemporary Turkey also involves the historical, sociological and political-economic analysis of Turkish politics through the methodological localization of Turkish governance at the intersection of global-regional-national-local interactions of Turkish politics, exceptional in its analytical and methodological richness and explanatory power[2]. The issues relevant to Turkey today, such as consolidating democracy, addressing problems related to economic development, improving its human rights situation and its foreign policy, in a historical context, allow comparisons with other countries in the world that developed late and reflect the complexity of Turkey's political and socio-economic developments. Turkey's modernization process started in the 19th century with all its elements, including secularization and westernization[3].

Russian Georgian conflict (2008)

The 2008 Russian Georgian war is often seen as a precursor to modern hybrid conflicts, although it also involved direct military confrontations. Before and during the military conflict, Georgia's digital infrastructure was repeatedly attacked by Distributed Denial of Service (DDoS) attacks, which affected communications and disrupted the Georgian government's ability to coordinate. Russia used the media to disseminate narratives justifying military intervention in South Ossetia and Abkhazia. These regions have been supported by Russia in their efforts to secede from Georgia, and Moscow has used this conflict to expand its influence in the region. The 2008 Russo-Georgian conflict, often referred to as the Russo-Georgian War, has been the subject of much analysis, historical accounts and political commentary. In the summer of 2008, a conflict that seemed to have started in the Georgian breakaway territory of South Ossetia escalated rapidly into the most important European security crisis of the last decade. The implications of the Russo-Georgian war will be understood differently, depending on how one tells the story of what happened and one's perspective on the wider context[4].

The short-lived war between Russia and Georgia in August 2008 seemed too many to be an unexpected bolt out of the blue that disappeared as quickly as it appeared. A small war that shook the world is a fascinating look at the collapse of relations between Russia and the West, the disintegration and decline of the Western Alliance itself, and the fate of Eastern Europe in a time of economic crisis[5]. The Caucasus is often treated as a side-plot in Russia's history or a mere gateway to Asia, the five-day war in Georgia, which turned into a major international crisis in 2008, proves that it is still a combustible region whose internal dynamics and history deserve a much more complex appreciation by the world at large[6]. Georgia emerged from the fall of the Soviet empire in 1991 with the promise of rapid economic and democratic reform. But that promise remains unfulfilled. Economic collapse, secessionist provocations, civil war and failure to escape the legacy of Soviet rule, culminating in the 2008 war with Russia, characterize a two-decade struggle to establish democratic institutions and consolidate statehood. A broader critical analysis of Georgia's recent political and economic development illustrates what its "transition" has meant not only for the state but also for its citizens. An authoritative and compelling exploration of Georgia since independence is essential for those interested in the post-Soviet world[7].

Conflicts in the Baltic region (Estonia, Latvia, Lithuania)

The Baltic countries, which have significant Russian populations, are often targets of Russian disinformation campaigns and cyber-attacks. Following a dispute over the relocation of a Soviet monument, Estonia was the target of massive cyber-attacks, targeting government institutions, banks and communication networks. These attacks are considered the first major cyber-attacks against a state. Russia has used media and

[1] Hüseyin Işikal, Oğuzhan Göksel, *Turkey's Relations with the Middle East: Political Encounters after the Arab Spring*, Springer, 2018, p. 97

[2] Ziya Öniş, Fuat E. Keyman, *Turkish Politics in a Changing World: Global Dynamics and Domestic Transformations*, Istanbul Bilgi University Yayinlari, 2007, p. 27

[3] Meliha Altunisik, Ozlem Tur, *Turkey: Challenges of Continuity and Change*, Routledge, 2022, p. 99

[4] Cornell E. Svante, Frederick S. Starr, *The Guns of August 2008: Russia's War in Georgia*, Routledge, 2009, p. 66

[5] Ronald Asmus, *Little War That Shook the World: Georgia, Russia, and the Future of the West*, St. Martin's Press, 2010, p. 18

[6] Thomas de Wall, *The Caucasus: An Introduction*, Oxford University Press, 2010, p. 39

[7] Jones F. Stephen, *Georgia: A Political History Since Independence*, I. B. Tauris, 2012, p. 88

social networks to disseminate narratives aimed at dividing Baltic societies and promoting Russian interests. The aim is often to sow mistrust between the Russian minority and the governments of these countries and to undermine solidarity within NATO and the EU. The Baltic region, which includes Estonia, Latvia and Lithuania, has had a rich and complex history, marked by conflicts, occupations and struggles for independence.

The world's attention has focused on the newly independent Baltic states of Latvia, Estonia and Lithuania, which are struggling to become politically and economically viable. The history and culture of the Baltic states, from their ancient origins to their contemporary status, their religious and racial differences, their relations with Russia and the West and their prospects for the future, their new constitutions and the 1992 elections, the current forces of law and order, the demolition of the Soviet economies and the possibilities of democracy and Europeanization or ethnic conflict and nationalist dictatorship, are of particular importance to our study[1]. Since the end of the Cold War there has been increased interest in the Baltic countries. Estonia, Latvia and Lithuania, after gaining independence, have developed at their own pace, with their own agendas and facing their own obstacles. There were many tensions accompanying a post-communist return to Europe after long years of separation and how each country responded to the demands of becoming a modern European state. Estonia was the first of the former Soviet republics to begin accession negotiations with the European Union in 1988 and is a potential candidate for the next round of EU enlargement in 2004. Lithuania and Latvia have also expressed their desire to become future members of NATO and the EU[2].

Russian interference in Western electoral processes

Russia has been accused of interfering in electoral processes in several Western countries, including in the US presidential election (2016) and elections in France and Germany. Through social media, Russian hacker groups spread fake news and polarizing narratives to influence voters and sow social discord. Russian-backed hacker groups, such as Cozy Bear and Fancy Bear, have carried out cyber-attacks on voting systems, political parties and critical infrastructure to obtain sensitive information or disrupt electoral processes. Russia's interference in Western electoral processes has been the subject of extensive research and analysis, especially after the major incidents of the 2010s. It is worth remembering the hacking of computer servers described as Watergate 2.0, where cyber thieves used everything: sensitive documents, emails, donor information, even voicemails. Western intelligence agencies traced the hack to Russian spy agencies and dubbed them “cyber bears”. Soon the media was flooded with stolen information, relayed via Julian Assange, the founder of WikiLeaks. It was a massive attack on America, but the Russian hackers seemed to have only one goal - the election of Donald J. Trump as president of the United States. Their goal? To end 240 years of free and fair American democratic elections[3]. Modern warfare is a war of narratives, where bullets are fired both physically and virtually. Whether you're a president or a terrorist, if you don't understand how to use the power of social media effectively, you may win a battle, but you will lose a 21st century war[4].

Another noteworthy example is the international intrigue, the cyber espionage, the superpower rivalry, which has led to Trump's strange relationship with Putin, the strange ties between members of his inner circle (including Paul Manafort and Michael Flynn) and Russia. That bizarre scandal explains the stakes and begets one of the biggest questions in American politics: how and why did a foreign government infiltrate the country's political process and gain influence in Washington?[5] With the end of the Cold War, the victory of liberal democracy seemed definitive. Russia had found allies among nationalists, oligarchs and radicals everywhere, and its desire to dissolve Western institutions, states and values resonated in the West itself. The rise of populism, the British vote against the EU and the election of Donald Trump were all Russian goals, but their realization reveals the vulnerability of Western societies. To understand the challenge is to see, and

[1] Anatol Lieven, *The Baltic Revolution: Estonia, Latvia and the Path to Independence*, Yale University Press, 1994, p. 17

[2] Thomas Lane, Artis Pabriks, Aldis Purs, David J. Smith, *The Baltic States: Estonia, Latvia and Lithuania*, Routledge, 2017, p. 19

[3] Malcolm Nance, *The Plot to hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election*, Skyhorse, 2016, p. 77

[4] David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century*, Basic Books, 2017, p. 101

[5] Michael Isikoff, Corn David, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*, Twelve, 2018, p. 13

perhaps renew, the fundamental political virtues offered by tradition and demanded by the future[1]. Examples such as poisoned dissidents, election interference, armed invasions, international treaties thrown into chaos, secret military reinforcements, hackers and viruses, weapons deployed in space are just a few examples of this conflict where certain actors are in the shadows and affected states are forced to adapt and fight back; the war of the future is already here with us[2].

Misinformation is as old as mankind. When Satan told Eve that nothing would happen if she bit the apple, that was misinformation. But the rise of social media has made disinformation even more pervasive and pernicious in our current age. In a disturbing turn of events, governments are increasingly using disinformation to create their own false narratives, and democracies are proving not very good at combating it. The information wars underline that we need to find a way to combat this growing threat to democracy[3]. We live in an age of disinformation, of organized deception. Intelligence agencies invest vast resources in hacking, leaking and falsifying data, often with the aim of weakening the very foundation of liberal democracy: trust in facts. The story of modern disinformation begins with the post-Russian Revolution confrontation between communism and capitalism that would define the Cold War. As misinformation develops, it is certain that we will live in a future of projected polarization, more active and less measured, and the tools needed to navigate through the deception[4].

The impact of hybrid warfare on the civilian population

Hybrid warfare has a profound and often devastating impact on civilians. The impact of hybrid warfare on civilians is a critical area of study that focuses on how this complex form of conflict affects populations in a variety of ways, including psychological stress, displacement and social disruption. Here's how hybrid warfare affects civilians:

Disruption of essential services

Cyber-attacks and physical attacks on critical infrastructure (electricity grids, water supplies and transportation networks) can lead to significant disruptions. These attacks often aim to cause chaos and undermine public confidence in the government. Disruption to economic activities, such as through ransomware attacks on businesses or supply chain disruptions, can lead to job losses, economic instability and increased living costs for civilians.

Spreading disinformation and propaganda

Misinformation campaigns can spread false or misleading information, creating confusion and fear among the population. Disinformation can deepen existing social divisions by promoting divisive narratives, leading to increased social polarization and fragmentation. This can damage community relations and make it more difficult to achieve social cohesion.

Psychological impact

The constant threat of cyber-attacks, disinformation and economic instability can contribute to widespread stress and anxiety among civilians. This psychological impact can be particularly severe in conflict zones or areas heavily affected by hybrid tactics. Prolonged exposure to hybrid warfare tactics, including violent incidents, disinformation and economic hardship, can lead to long-term mental health problems, including trauma, depression and PTSD (Post-traumatic stress disorder).

Impact on public services and governance

Hybrid warfare tactics such as disinformation and political subversion can erode trust in public institutions and government authorities. This can lead to decreased public confidence in the effectiveness and legitimacy of government responses. Disruption and undermining efforts can lead to weak governance, making it more difficult for governments to deliver essential services and maintain law and order. This can lead to a decline in public safety and overall quality of life.

[1] Timothy Snyder, *The Road to Unfreedom: Russia, Europe, America*, Crown, 2018, p. 92

[2] Jim Sciutto, *The Shadow War: Inside Russia's and China's Secret Operations to Defeat America*, Harper, 2019, p. 67

[3] Richard Stengel, *Information Wars: How We Lost the Global battle Against Disinformation and What We Can Do About It*, Atlantic Monthly Press, 2019, p. 81

[4] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, Farrar, Straus and Giroux, 2020, p. 17

Economic hardship

Civilians may face higher living costs due to economic disruptions such as inflation or shortages of goods and services. This can lead to financial strain, especially for vulnerable populations. Disruption to businesses and industries, including through cyber-attacks and economic sanctions, can lead to job losses and reduced economic opportunities, further affecting civilian livelihoods.

Physical safety and security

Hybrid warfare can include the use of irregular forces, terrorists and proxy groups, which can directly target civilians through attacks, bombings and other forms of violence. This can lead to casualties and displacement. Civilians in conflict or targeted areas may become more vulnerable to violence, exploitation and human rights violations. The mix of conventional and non-conventional tactics can make it harder to protect civilians.

Displacement and refugee crises

Conflict and instability resulting from hybrid wars can lead to large-scale displacement of civilians, creating refugee crises and putting pressure on neighbouring countries and international aid organizations. Displaced populations often face serious humanitarian needs, including access to shelter, food, healthcare and education. Addressing these needs can be difficult in the context of an ongoing hybrid war.

Cultural and social impact

In some cases, hybrid warfare tactics may target cultural and historical sites with the aim of eroding cultural identity and heritage. This can have lasting effects on communities and their sense of identity. The societal divisions exacerbated by hybrid warfare tactics can lead to social disintegration, making it more difficult for communities to function cohesively and support each other.

Legal and ethical implications

Tactics used in hybrid warfare can lead to various human rights violations, including arbitrary detention, torture and other forms of ill-treatment. These violations can be committed by both state and non-state actors. The combination of conventional and unconventional tactics can complicate efforts to hold perpetrators accountable, leading to a lack of justice for victims of hybrid warfare. Hybrid warfare has been an integral part of the historical landscape since antiquity, but it is only recently that analysts have incorrectly labeled these conflicts as unique. Throughout history, great powers have faced adversaries who have used a combination of regular and irregular forces to nullify the advantage of the great power's superior conventional military force. Hybrid wars are labor-intensive and long-term affairs; they are difficult battles that defy the internal logic of opinion polls and election cycles. Hybrid wars are also the most likely conflicts of the 21st century, as competitors use hybrid forces to deplete military capabilities in protracted campaigns of exhaustion[1].

Behind the physical nature of the tumult of war are structural forces that create landscapes of civilian vulnerability. These forces operate in four sectors of modern warfare: nationalist ideology, state-sponsored armies, global media and international institutions. Each sector promotes its own constructions of civilian identity in relation to militant combatants: constructions that prove lethal to non-combatant civilians who lack political power and decision-making capacity over their own survival. Civilians and Modern Warfare offers a critical perspective on the plight of civilians in war, examining the political and normative underpinnings of the decisions, actions, policies and practices of major sectors of war. The contributors seek to undermine the 'tunnel effect' of the militarist framework in terms of the experiences of non-combatants[2].

Hybrid warfare refers to a military strategy that combines conventional warfare, so-called 'irregular warfare' and cyber-attacks with other methods of influence, such as fake news, diplomacy and foreign political intervention. As hybrid warfare becomes increasingly commonplace, there is an imminent need for research to draw attention to how these challenges can be addressed to develop a comprehensive approach to hybrid threats and hybrid warfare[3].

[1] Williamson Murray, Peter R. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, 2012, p.75

[2] Daniel Rothbart, Karina K. Korostelina, Cherkaoui, Mohammed, *Civilians and Modern War: Armed Conflict and the Ideology of Violence (War, Conflict and Ethics)*, Routledge, 2012, p. 18

[3] Mikael Weissmann, Nikolas Nilson, Björn Palmertz, Thunholm Per, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, I. B. Tauris, 2021, p. 93

Ethics of using weapons with artificial intelligence

The ethics of AI weapons is a complex and controversial issue, involving a range of moral, legal and practical considerations. Once activated, AI weapons, often referred to as autonomous weapon systems (AWS), can operate independently of human intervention, making targeting and engagement decisions on their own. This raises several ethical issues:

Responsibility and accountability

One of the main ethical concerns is the question of liability. If an autonomous weapon causes unintentional harm, who is responsible? Is it the programmer, the manufacturer, the military commander, or the machine itself? Lack of clear accountability could lead to situations where no one is held responsible for wrongful death or destruction, undermining the principle of justice.

Human dignity and moral agency

Autonomous weapons can undermine human dignity by removing human moral agency from the decision to take life. The decision to kill has profound moral implications and many argue that it should remain under human control. Allowing machines to make life and death decisions could be considered dehumanizing and ethically unacceptable.

Distinction and proportionality

In armed conflict, the principles of distinction and proportionality are fundamental to the laws of war. Distinction requires that combatants distinguish between military targets and civilians, while proportionality requires that the harm caused by military action be proportionate to the military advantage gained. There are concerns that AI weapons may have difficulty making these complex ethical judgments, leading to indiscriminate or disproportionate attacks.

Risk of escalation

Weapons with artificial intelligence could lower the threshold for conflict, making it easier for states or non-state actors to initiate violence. The speed and efficiency of autonomous systems could lead to the rapid escalation of conflicts, reducing the time available for diplomacy and peaceful resolution. In addition, the use of AI weapons by one state could provoke an arms race as other states develop similar or more advanced systems.

Unintended consequences

Autonomous weapon systems could behave unpredictably or malfunction in ways that cause unintended harm. The complexity of artificial intelligence systems makes it difficult to foresee all possible scenarios, leading to the risk of accidents or unintended escalations. Moreover, these systems could be hacked or reused by malicious actors, which poses significant security risks.

Potential for abuse

AI weapons could be used for oppressive purposes, such as targeting political dissidents, suppressing protests or carrying out targeted assassinations without due process. The availability of such technology could allow authoritarian regimes or non-state actors to commit acts of violence with impunity, thus exacerbating human rights violations.

Legal and regulatory challenges

The development and use of AI weapons challenges existing legal frameworks, including International Humanitarian Law (IHL) and human rights law. Current legislation is not fully prepared to address the complexities of autonomous systems and there is a lack of consensus on how to regulate these weapons. Some advocate a pre-emptive ban, while others advocate stricter controls and oversight.

Ethical justifications for AI weapons

Proponents of AI weapons argue that they could reduce harm in warfare by being more accurate and effective than human soldiers. For example, AI systems could be designed to more effectively avoid collateral damage or carry out dangerous missions without risking human lives. However, these potential benefits must be balanced against significant risks and ethical challenges.

Bias and discrimination

Artificial intelligence systems are only as good as the data on which they are trained, and if that data is biased, the AI's decisions may also be biased. In the context of guns, this could lead to discriminatory targeting based on race, ethnicity or other factors. This raises serious ethical questions about fairness and the potential for AI to perpetuate or exacerbate existing injustices.

Global security and stability

The proliferation of AI weapons could destabilize global security. If more states develop and deploy such systems, this could lead to a new form of arms race, where the focus is on developing increasingly autonomous and lethal technologies. This could increase the likelihood of accidental or deliberate conflicts with potentially catastrophic consequences. AI weapons ethics is a complex and evolving topic, and several books explore it from different angles. Military robots and other potentially autonomous robotic systems such as unmanned combat aerial vehicles (UCAVs) and unmanned ground vehicles (UGVs) could soon be introduced to the battlefield. Looking further into the future, we could see autonomous micro- and nanorobots armed and deployed in swarms of thousands or even millions. This increasing automation of warfare could come to represent a major discontinuity in the history of warfare: humans will first be removed from the battlefield and one day may even be largely excluded from the decision-making cycle in the future high-tech, high-speed robotic warfare of the future. While the current technological problems will undoubtedly be overcome, the biggest obstacles to the use of automated weapons on the battlefield are likely to be legal and ethical concerns[1].

Prominent experts in science and the humanities examine aspects of robot ethics ranging from sex to war. Today, robots fulfill many roles, from entertainer to educator to executioner. As robotic technology advances, ethical concerns become more pressing: Should robots be programmed to follow an ethical code, if possible? Are there risks in forming emotional bonds with robots? How might society and ethics change with robotics? Ethics often lags technological developments[2]. The discussion on lethal autonomous weapon systems (LAWS) centers on the ethics of allowing a computer to decide to kill (or not to kill) a human being. Much of the current discourse on autonomous weapons stems from concern about the ethical implications. Efforts are currently being made to institute laws and regulations that would inhibit or eliminate the use of LAWS[3]. The ethical questions are *to what extent should such technologies be advanced*? *And if responsible democracies ban them, would they prevent rogue regimes from profiting from them*? At the forefront of a game-changing debate. When the choice is life or death, the human heart cannot be replaced[4].

Artificial intelligence is playing a growing role in military weapons systems. Going beyond the bomb-carrying drones used in the war in Afghanistan, the Pentagon is now in a race with China and Russia to develop "lethal autonomous weapon systems" (LAWS). While the use of robotic systems could reduce military casualties in a conflict, a major concern is: should we allow machines to make life-and-death decisions in combat? Other areas of concern include the following: who would be responsible for the actions of fully autonomous weapons - the programmer, the machine itself, or the country implementing LAWS? When war becomes just a matter of technology, will war become more likely, bringing humanity closer to annihilation? What will happen if artificial intelligence technology reaches a "singularity level" such that our weapons are controlled by an intelligence that surpasses human intelligence?[5]

The question of whether new rules or regulations are needed to regulate, restrict or even prohibit the use of autonomous weapon systems has been the subject of debate lately, so society needs to invest in difficult discussions that address the ethics, morality and law of these new digital technologies and understand the human role in their creation and operation[6]. Artificial intelligence is the most talked about and arguably the most powerful technology in the world today. The very rapid development of this technology and its power to change the world and perhaps even us call for a serious and systematic reflection on its ethical and social implications and on how its development should be directed[7].

Autonomous weapon systems seem to be on the way to becoming accepted technologies of war. The weaponization of artificial intelligence raises questions about the continued control of human beings over the

[1] Armin Krishnan Killer, *Robots: Legality and Ethicality of Autonomous Weapons*, Routledge, 2009, p. 77

[2] Patrick Lin, Keith Abney, George A. Bekey, *Robot Ethics: The Ethical and Social Implications of Robotics*, The MIT Press, 2014, p. 103

[3] Ted W. Schroeder, *Lethal Autonomous Weapon Systems in Future Conflicts*, Independently Published, 2017, p. 22

[4] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton & Company, 2018, p. 81

[5] Louis A. del Monte, *Genius Weapons: Artificial Intelligence, Autonomous Weaponry, and the Future of Warfare*, Prometheus, 2018, p.97

[6] Jai Galliot, Duncan MacIntosh, Jens David Ohlin, *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare (Ethics, National Security, and the Rule of Law)*, Oxford University Press, 2021, p. 89

[7] Soraj Hongladarom, *The Ethics of AI and Robotics: A Buddhist Viewpoint*, Lexington Books, 2021, p. 88

use of force. The notion of meaningful human control has become a central point of international debate on lethal autonomous weapons systems among members of the United Nations: many states have divergent ideas about various complex forms of human-machine interaction and the point at which human control ceases to be meaningful[1].

Regulating the use of autonomous weapon systems (AWS)

Regulating autonomous weapon systems (AWS) is a complex challenge that requires a multidimensional approach, involving legal, ethical, technical and international dimensions. Here are some key strategies and considerations for regulating AWS:

International legal framework

One of the main ways of regulating AWS is the establishment of new international treaties specifically addressing their development, deployment and use. Such treaties could establish clear rules and guidelines, like existing arms control agreements such as the Chemical Weapons Convention. Existing International Humanitarian Law (IHL), such as the Geneva Conventions, could be updated or reinterpreted to respond to the unique challenges posed by AWS. This could include clarifying the application of principles such as distinction, proportionality and accountability in the context of autonomous systems.

Definition and classification

A major regulatory challenge is defining what constitutes an AWS. Clear and precise definitions are essential to ensure that regulations target the systems concerned without stifling legitimate technological advances. Definitions should distinguish between different levels of autonomy and specify the characteristics that make a system subject to regulation. AWS could be categorized according to their level of autonomy, potential for harm, and intended use (e.g. lethal vs. non-lethal). This categorization could help tailor regulations to different types of systems, ensuring that the most dangerous systems are subject to the most stringent controls.

Development and testing standards

Regulations could require rigorous testing of the safety and reliability of AWS systems before they are deployed. This would involve ensuring that the systems can operate within the limits required by international law and do not pose unreasonable risks of malfunction or unintended harm. Developers of AWS should be required to document and disclose the processes used to train and test their systems, including the datasets used and the decision-making criteria. This transparency would help ensure that AWS is designed and tested with ethical considerations in mind.

Human control and supervision

Regulations could require that humans remain in the decision-making loop for critical functions, especially those involving the use of lethal force. This could involve requiring human confirmation before an AWS engages a target. Even for systems that operate autonomously, mechanisms should be in place to ensure human oversight and accountability. Regulations could specify who is responsible for the actions of an AWS, including the roles of commanders, operators and developers.

Ethical guidelines and codes of conduct

Governments, international organizations and industry groups could develop ethical frameworks to guide the development and use of AWS. These could include principles such as respect for human dignity, the need to minimize harm, and the importance of maintaining human control over critical decisions. AWS developers and operators could be required to adhere to codes of conduct that align with these ethical frameworks. These codes could include commitments to transparency, accountability and avoid civilian harm.

International cooperation and standards

Some proponents propose a global moratorium on the development and deployment of AWS until a comprehensive regulatory framework is in place. This would prevent a potential arms race and allow time for international discussions on how best to regulate these systems. To build confidence and prevent escalations, States could engage in confidence-building measures, such as sharing information on their AWS programs, participating in joint exercises, and engaging in mutual verification processes.

Export control and non-proliferation

[1] Hendrik Huelss, Ingvild Bode, *Autonomous Weapons Systems and International Norms*, McGill-Queen's University Press, 2022, p. 84

Regulations could impose strict controls on the export of AWS and related technologies, especially to conflict regions or actors with a poor human rights record. This would help prevent proliferation of these systems to irresponsible or dangerous parties. States could negotiate non-proliferation agreements that limit the spread of AWS technologies and prevent their use in violation of international law.

Public and stakeholder involvement

Governments and international bodies should work with the public, civil society and experts in AI, ethics and international law to gather input on VAS regulation. Public consultation can help ensure that regulations reflect societal values and concerns. Regulation should involve collaboration between governments, the private sector, academia and civil society. This multi-stakeholder approach can help ensure that regulations are based on diverse perspectives and expertise.

Liability mechanisms

The regulations should establish clear mechanisms of legal liability for the use of AWS. These could include provisions for holding individuals or entities legally liable for unlawful use of AWS, whether through criminal prosecution, civil liability or other legal means. Some have proposed the creation of an international tribunal or special oversight body for AWS-related incidents. This body could investigate alleged violations of international law and provide a forum for dispute resolution.

Research and development safeguards

Institutions involved in AWS research and development could be required to establish ethical review boards to assess the potential impact of their work. These panels could ensure that R&D activities comply with ethical standards and do not contribute to the development of harmful or illegal technologies. Regulation should address the dual-use nature of AI technologies, which can be used for both civilian and military purposes. There should be safeguards to prevent the misuse of AI research for the development of autonomous weapons. Regulating autonomous weapon systems (AWS) is a crucial and complex topic. Artificial intelligence helps you choose what books you buy, what movies you see and even who you date. It puts "intelligence" into your smartphone and will soon be driving your car. But artificial intelligence could also threaten our very existence. Scientists argue that once artificial intelligence reaches this level, it will have survival needs like ours. We could be forced to compete with a rival more cunning, powerful and alien than we can imagine[1].

Stories about unmanned vehicles are now regularly in the national news, and not always in a good way. When utilized in military operations, autonomous weapon systems (AWS) have the potential to save lives as well as apply lethal force on land, at sea and in the air. The development of AWS policy and doctrine should characterize autonomy not as a discrete property of a particular system, but rather as a function that varies with the strategic, operational and tactical context and mission application. AWS design, planning, and operations should be tempered by intentional consideration of human judgment and control, as well as legal and ethical standards that promote international credibility[2].

Over the past decade, armed drones have entered the military arsenal as a basic tactic to combat terrorism. When combined with access to reliable intelligence, they make it possible to deploy a lethal force accurately across borders while keeping your own soldiers out of harm's way. The ability to direct force with great precision also offers the possibility of reducing civilian harm. At the same time, because drones remove some of the traditional constraints on the use of force, such as the need to gain political support for full mobilization, they lower the threshold for launching military strikes. The development of drone capabilities in dozens of countries increases the need for global standards on the use of these weapons to ensure that their use is strategically wise and ethically and legally sound[3].

[1] James Barrar, *Our Final Intervention: Artificial Intelligence and the End of the Human Era*, Thomas Dunne Books, 2013, p. 79

[2] Jeffrey L. Caton, *Autonomous Weapon Systems: A Brief Survey of Developmental, Operational, Legal, and Ethical Issues*, 2015, p. 53

[3] David R. T. Gardner, *Drones and the Future of Armed Conflict: Ethical, Legal, and Strategic Implications*, University of Chicago Press, 2015, p. 97

The future of artificial intelligence ethics

The future of AI ethics is poised to become increasingly critical as artificial intelligence continues to evolve and integrate more deeply into society. Here are some key trends and considerations that will likely shape the future of AI ethics:

Evolution of ethical frameworks

As AI systems become more advanced and are used in a wider range of contexts, ethical frameworks will need to evolve dynamically. These frameworks need to adapt to new applications, societal changes and cultural differences. Ethical considerations will increasingly need to consider the specific contexts in which AI is used, such as healthcare, law enforcement, finance and privacy. The future of AI ethics will involve greater collaboration between ethicists, technologists, policy makers and other stakeholders. Inter-disciplinary approaches will be essential to address the complex ethical challenges raised by AI, ensuring the integration of ethical considerations throughout the AI development process.

IA governance and regulation

The development of international standards and agreements will be essential to regulate the ethical use of AI across borders. This could involve the creation of global regulatory bodies or agreements that establish basic ethical standards and best practices for the development and implementation of AI. AI regulation will need to be responsive and adaptive to keep pace with technological advances. This could involve the use of regulatory sandboxes where new AI technologies can be tested in a controlled environment, allowing regulators to better understand their implications and refine regulation accordingly.

The ethics of artificial intelligence in decision-making

As AI systems increasingly make decisions that have an impact on people's lives, there will be a growing emphasis on transparency and explainability. People affected by AI-driven decisions will demand to know how those decisions are made and ensuring that AI systems are interpretable will become a key ethical priority. Addressing bias and ensuring fairness in AI decision-making will remain a central ethical challenge. Future efforts are likely to focus on developing more sophisticated techniques to detect, mitigate and prevent bias in AI systems, as well as on ensuring that AI-based decisions do not perpetuate or exacerbate social inequalities.

Ethical AI in the workforce

As AI continues to automate tasks and transform industries, ethical considerations related to the impact on employment will become more pressing. Policymakers and businesses will need to address issues such as job displacement, retraining, and the creation of new opportunities to ensure that the benefits of AI are distributed. The future of work will increasingly involve collaboration between humans and AI. Ethical guidelines will be needed to ensure that this collaboration respects human dignity, promotes worker autonomy, and does not lead to exploitation or over-reliance on AI systems.

AI and privacy

As AI systems rely heavily on data, ensuring the collection, use and ethical protection of personal data will be a key concern. Future ethical frameworks will need to address issues of consent, data ownership and the potential for AI to infringe on individual privacy rights. The use of AI in surveillance raises significant ethical issues, particularly in relation to privacy, autonomy and potential misuse by governments or corporations. Balancing the benefits of AI-based surveillance with the need to protect civil liberties will be an ongoing ethical challenge.

Ethics of autonomous systems

The ethical implications of autonomous weapons will continue to be a major topic of debate. The future is likely to see increased efforts to regulate or even ban these systems, with a focus on ensuring that decisions to use lethal force remain under human control. As autonomous vehicles and other artificial intelligence systems become more prevalent in public spaces, ethical considerations will need to address issues such as safety, liability, and impact on public infrastructure. Ensuring that these systems operate safely and fairly will be a priority.

AI and the ethical development of AI

Future AI ethics will increasingly focus on integrating ethical considerations directly into the design and development of AI systems. This could involve the use of ethical impact assessments, incorporating ethical principles into AI algorithms, and adopting design practices that prioritize the welfare of the user and the good of society. Companies developing AI technologies will face increasing pressure to adhere to ethical standards and demonstrate their commitment to responsible AI practices. This could include transparency in AI development, accountability for AI-related harms and efforts to ensure that AI benefits society as a whole.

AI and human rights

AI has the potential to exacerbate existing inequalities, and future ethical frameworks will need to address the impact of AI on marginalized and vulnerable populations. This could involve ensuring that AI systems are inclusive, do not discriminate and contribute to social justice. The use of AI in areas such as surveillance, predictive policing and social scoring systems pose significant threats to individual freedoms and human rights. The ethical development of AI will need to prioritize the protection of human rights and the prevention of the use of AI as a tool of oppression.

Ethics of artificial intelligence in healthcare

As AI is increasingly used in healthcare for diagnostics, treatment planning and personalized medicine, ethical considerations related to patient confidentiality and informed consent will become more important. Ensuring that AI-based healthcare respects patient autonomy and confidentiality will be essential. AI has the potential to improve healthcare outcomes, but risks widening disparities in access to care. Ethical frameworks will need to address how AI can be used to promote equitable access to care and improve outcomes for all patients.

Public involvement and education

The future of AI ethics will involve greater efforts to engage the public in discussions about the ethical implications of AI. This includes educating people about how AI systems work, the potential risks and benefits, and their rights in an AI-driven world. It will be important to ensure that the development of AI ethics is inclusive and reflects diverse perspectives. This could involve creating platforms for public input, ensuring that underrepresented voices are heard and promoting a more democratic approach to AI governance.

Exploring the future of AI ethics is a fascinating and crucial area of study given the rapid advances in AI technologies. In the popular imagination, superhuman artificial intelligence is a coming wave that threatens not just human jobs and relationships, but civilization itself. Conflict between humans and machines is seen as inevitable, and its outcome is all too predictable[1]. What is certain is that we will all need to understand the enormous potential of artificial intelligence to transform our daily lives, but also how our lives will be shaped by artificial intelligence[2].

The impact of artificial intelligence on hybrid conflicts in the 21st century

Artificial Intelligence (AI) has significantly influenced hybrid conflicts in the 21st century, with both advantages and disadvantages. Hybrid conflicts are complex, involving a mix of conventional military tactics, irregular warfare, cyber operations and political subversion. We are just beginning to see a massive change in military technology. As these technologies proliferate, they will have profound effects both on the front line and on politics at home. Removing humans from the battlefield makes wars easier to start but more complex to fight. Replacing men with machines may save some lives but will reduce morale and psychological barriers to killing. The "warrior ethic" that has long defined the identity of soldiers will erode, as will the laws of war that have governed military conflicts for generations. Paradoxically, these new technologies will bring war to our doorstep. The future of war is as fascinating as it is terrifying[3]. Due to unprecedented developments in artificial intelligence, dramatic changes will take place much sooner than many of us expected. Most experts are already saying that AI will have a devastating impact on jobs for workers. The jobs that will be affected and over how long, the jobs that can be improved with AI and, most importantly, how we can provide solutions to some of the most profound changes in the future of human history[4]. The heady optimism of the early days of the internet has turned dark. The fight for a humane future has never been more urgent. We still have the power to decide what kind of world we want to live in[5].

[1] Stuart Russell, *Human Compatible: Artificial Intelligence and the Problem of Control*, Viking, 2019, p. 66

[2] Kai-Fu Lee, Chen Quifan, *AI 2041: Ten Visions for Our Future*, Crown Currency, 2021, p. 37

[3] Peter Singer, *Warren, Wired for War: The Robotics revolution and Conflict in the 21st Century*, Penguin Books, 2009, p. 67

[4] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order*, Harper Business, 2018, p. 57

[5] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019, p. 79

As a general-purpose and dual-purpose technology, artificial intelligence can be used for both good and bad. The use of artificial intelligence is becoming increasingly important to the government's mission to keep its nations safe. However, the design, development and use of AI for national security raises a wide range of legal, ethical, moral and privacy issues. In examining the contradictory uses of AI, some countries use AI to launch disinformation attacks by automating the creation of false or misleading information to undermine public discourse[1].

1. Advantages of using artificial intelligence in hybrid conflicts

Enhanced surveillance and intelligence gathering

Artificial intelligence can process large amounts of data from various sources, such as social media, satellite imagery and communication intercepts, to identify patterns and potential threats. This helps in taking preventive measures and situational awareness. AI models can predict enemy movements and intentions by analyzing historical data and current trends, thus improving strategic planning.

Improved cyber capabilities

AI systems can automatically detect and respond to cyber threats, strengthening defenses against hacking and cyber-espionage. Artificial intelligence can be used to develop sophisticated malware or execute cyber-attacks with high precision, disrupting adversaries' communications and infrastructure.

Autonomous systems

Artificial intelligence-powered drones and robotic systems can perform reconnaissance, deliver payloads or engage in combat with minimal human intervention, reducing the risk to personnel. AI can optimize logistics and supply chains, improving the efficiency of military operations and resource allocation.

Enhanced information warfare

AI can rapidly generate and spread disinformation, influencing public opinion and destabilizing societies. This can be used to manipulate perceptions and sow discord among adversaries. AI algorithms can amplify certain narratives or suppress others, shaping the information environment in favor of one side.

2. Disadvantages of artificial intelligence in hybrid conflicts

Ethical and legal concerns

The use of AI in autonomous weapons raises ethical concerns such as the potential for unintended escalation and lack of accountability for actions taken by machines. AI-based operations, particularly in cyber warfare, can unintentionally damage civilian infrastructure, leading to collateral damage and humanitarian crises.

Vulnerability to AI manipulation

AI systems themselves can be vulnerable to adversarial attacks, where slight manipulations of input data can cause the AI to make incorrect decisions or predictions.AI systems can inherit biases from their training data, which can lead to faulty intelligence and decision making.

Escalation risks

The speed and scale at which artificial intelligence can operate could lead to the rapid escalation of conflicts, as automated systems can act faster than human surveillance can manage. The development of advanced artificial intelligence in military applications may trigger an arms race, with nations competing to outdo each other in artificial intelligence capabilities, increasing global tensions.

Over-reliance and over-reliance

Over-reliance on AI systems can lead to vulnerabilities if these systems malfunction or are compromised. Human oversight is essential to mitigate these risks. Over-reliance on artificial intelligence could erode human judgment and critical decision-making, leading to less adaptive responses in unpredictable situations.

In short, while AI offers significant advantages in improving capabilities and effectiveness in hybrid conflicts, it also introduces new risks and ethical dilemmas. Balancing the benefits with the potential drawbacks is essential to ensure that AI contributes positively to security and stability, rather than exacerbating conflict.

[1] Reza Montasari, *Artificial Intelligence and national Security*, Springer, 2022, p. 91

International law rules for and against the use of artificial intelligence in hybrid conflicts in the 21st century

International law on the use of artificial intelligence (AI) in hybrid conflict is still developing, reflecting the rapidly evolving nature of the technology and its application in military and non-military domains. There are aspects of existing international law that can be interpreted as favorable or restrictive to the use of AI in such contexts. Here is a breakdown of these perspectives:

Existing legal frameworks supporting the use of AI

- Principle of state sovereignty and self-defense:

Article 51 of the UN Charter. This article allows states the right to self-defense if they are attacked. AI-driven defensive systems, such as automated cybersecurity measures, can be considered legitimate tools for protecting a nation's infrastructure.

Law of Armed Conflict (LOAC)/International Humanitarian Law (IHL). AI technologies that comply with the principles of LOAC, such as distinction (differentiating between combatants and non-combatants) and proportionality (ensuring that harm to civilians is minimized), may be permitted. For example, AI could be used for improved targeting and reduced collateral damage in military operations.

- Cybersecurity and defense norms:

Tallinn Manual on the International Law Applicable to Cyber Warfare. While not legally binding, this manual provides guidance on how existing international law might apply to cyber operations, including the use of AI. It suggests that states can use AI for cyber defense as long as it respects the norms of sovereignty and proportionality.

Legal and ethical constraints on the use of AI

- Geneva Conventions:

The Geneva Conventions and their Additional Protocols regulate conduct during armed conflicts, emphasizing the protection of civilians. AI systems used in warfare must comply with these conventions by ensuring they can distinguish between legitimate military targets and protected civilians.

Article 36 of Additional Protocol I. Requires states to review new weapons, methods, or means of warfare to ensure they are not prohibited by international law. This would apply to autonomous AI systems and lethal autonomous weapon systems (LAWS).

- Human rights law:

International Covenant on Civil and Political Rights (ICCPR). Ensures the right to life and prohibits arbitrary deprivation of life. The use of AI in hybrid conflicts, especially in autonomous weapons systems, must be designed and used in a way that upholds these principles.

- Ethical constraints on autonomous systems:

"Meaningful Human Control" Doctrine. Many international bodies, including the UN and advocacy groups, argue that any AI system capable of lethal action should operate under meaningful human oversight. The use of AI in decision-making without human control raises serious ethical and legal concerns.

UN Group of Governmental Experts on LAWS. This group has discussed the implications of autonomous weaponry, recommending restrictions to ensure that humans remain responsible for life-or-death decisions.

Potential Violations and Concerns

- Accountability and attribution.

One of the primary concerns is how to attribute responsibility for actions taken by AI systems. If an autonomous AI system acts outside the bounds of international law or commits an unlawful act, it can be difficult to determine who is legally accountable—the state, the manufacturer, or the operator.

- Discrimination and bias:

AI systems can inherit biases from their training data, leading to potential discrimination in targeting or operational errors. This can violate the principle of distinction and potentially result in disproportionate harm to civilians.

- Cyber operations and AI:

The use of AI in cyber-attacks poses legal challenges regarding sovereignty and the prohibition against non-consensual interference in the internal affairs of states (Article 2(4) of the UN Charter). AI-driven cyber operations that result in significant damage to a state's infrastructure or economy may be considered an act of aggression.

International Calls for Regulation

·UN and International Advocacy:

The United Nations, through various arms such as the UN Institute for Disarmament Research (UNIDIR), has called for discussions around AI and autonomous systems, promoting international norms and possibly new treaties to regulate their use.

·Campaign to Stop Killer Robots:

This international coalition advocates for a preemptive ban on fully autonomous weapons to ensure that decisions involving the use of force remain under human control.

·Global Partnership on AI (GPAI):

GPAI is an international initiative aimed at responsible AI use. Although not directly related to hybrid warfare, it promotes guidelines that can influence the development and use of AI in defense.

Emerging Legal and Policy Gaps

·Absence of Specific Treaties:

Currently, there is no binding international treaty specifically regulating the use of AI in hybrid conflicts. The laws that do apply are extrapolated from general principles of international humanitarian and human rights law.

·Rapid Technological Advancements:

The pace of AI development often outstrips the creation and implementation of laws and regulations. This creates a gap where states and non-state actors can leverage AI in ways that may not yet be fully addressed by existing legal frameworks.

Although international law provides some structure for the use of AI in conflict through general principles of international humanitarian law and human rights law, significant legal and regulatory gaps remain, particularly in the areas of accountability, the use of lethal autonomous systems and cyber operations. Efforts to establish new treaties or agreements specific to AI and hybrid warfare are ongoing, but the international community faces challenges in keeping pace with rapid technological advances.

Bibliography

Books

1. Altunisik, Meliha; Tur, Ozlem, *Turkey: Challenges of Continuity and Change*, Routledge, 2022
2. Applebaum, Anne, *Red Famine: Stalin's War on Ukraine*, Doubleday, 2017
3. Asmus, Ronald, *Little War That Shook the World: Georgia, Russia, and the Future of the West*, St. Martin's Press, 2010
4. Bajoghli, Narges, *Iran Reframed: Anxieties of Power in the Islamic Republic*, Stanford University Press, 2019
5. Barkey, Henry, J., *Reluctant Neighbor: Turkey's Role in the Middle East*, United States Institute of Peace, 1997
6. Barrar, James, *Our Final Intervention: Artificial Intelligence and the End of the Human Era*, Thomas Dunne Books, 2013
7. Barto, Andrew, G.; Sutton, Richard, S., *Reinforcement Learning: An Introduction*, Bradford Books, 2018
8. Beebe, George, *The Russia Trap: How Our Shadow War with Russia Could Spiral into Catastrophe*, Thomas Dunne, 2019
9. Berman, Ilan; Humire, Joseph, M., *Iran's Strategic Penetration of Latin America*, Lexington Books, 2016
10. Bostrom, Nick, *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press, 2016
11. Caton, Jeffrey, L., *Autonomous Weapon Systems: A Brief Survey of Developmental, Operational, Legal, and Ethical Issues*, lulu.com, 2015
12. Coeckelbergh, Mark, *AI Ethics*, The MIT Press, 2020
13. Cornell, Svante, E.; Starr, Frederick, S., *The Guns of August 2008: Russia's War in Georgia*, Routledge, 2009
14. Corr, Andreas, *Great Powers, Grand Strategies: The New Game in the South China Sea*, Naval Institute Press, 2018
15. Crist, David, *The Twilight War: The Secret History of America's Thirty-Year Conflict with Iran*, Penguin Publishing Group, 2013

16. de Wall, Thomas, *The Caucasus: An Introduction*, Oxford University Press, 2010
17. Demir, Ýdris, *Turkey's Foreign Policy Towards the Middle East: Under the Shadow of the Arab*, Cambridge Scholars Publishing, 2016
18. Dewan, Sandeep, *China's Maritime Ambitions and the PLA Navy*, Vij Books India, 2013
19. Erickson, Andrew, S.; Goldstein, Lyle, J.; Li, Nan, *China, the United States, and 21st-Century Sea Power: Defining a maritime Security Partnership*, Naval Institute Press, 2010
20. Freedman, Lawrence, *Ukraine and the Art of Strategy*, Oxford University Press, 2019
21. Galeotti, Mark, *Putin's Wars: From Chechnya to Ukraine*, Osprey Publishing, 2022
22. Galliot, Jai; MacIntosh, Duncan; Ohlin, Jens, David, *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare (Ethics, National Security, and the Rule of Law)*, Oxford University Press, 2021
23. Gardner, David, R., T., *Drones and the Future of Armed Conflict: Ethical, Legal, and Strategic Implications*, University of Chicago Press, 2015
24. Géron, Aurélien, *Hands-On Machine Learning with Scikit-Learn, Keras, And TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, O'Reilly Media, 2019
25. Goodfellow, Ian; Bengio, Yoshua, Courville, *Deep Learning*, The MIT Press, 2016
26. Hayton, Bill, *The South China Sea: The Struggle for Power in Asia*, Yale University Press, 2014
27. Hongladarom, Soraj, *The Ethics of AI and Robotics: A Buddhist Viewpoint*, Lexington Books, 2021
28. Huelss, Hendrik; Bode, Ingvild, *Autonomous Weapons Systems and International Norms*, McGill-Queen's University Press, 2022
29. Işikal, Hüseyin; Göksel, Oğuzhan, *Turkey's Relations with the Middle East: Political Encounters after the Arab Spring*, Springer, 2018
30. Isikoff, Michael; Corn, David, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*, Twelve, 2018
31. Jones, Stephen, F., *Georgia: A Political History Since Independence*, I. B. Tauris, 2012
32. Kaplan, Fred, *Dark Territory: The Secret History of Cyber War*, Simon & Schuster, 2017
33. Kaplan, Robert, D., *Asia's Cauldron: The South China and the End of a Stable Pacific*, Random House Trade Papperbacks, 2015
34. Kösebalaban, Hasan, *Turkish Foreign Policy: Islam, Nationalism, and Globalization (Middle East Today)*, Palgrave Macmillan, 2011
35. Krishnan, Armin, *Killer Robots: Legality and Ethicality of Autonomous Weapons*, Routledge, 2009
36. Lane, Thomas; Pabriks, Artis; Purs, Aldis; Smith, David, J., *The Baltic States: Estonia, Latvia and Lithuania*, Routledge, 2017
37. Lee, Kai-Fu, *AI Superpowers: China, Silicon Valley, and the New World Order*, Harper Business, 2018
38. Lee, Kai-Fu, Quifan, Chen, *AI 2041: Ten Visions for Our Future*, Crown Currency, 2021
39. Lieven, Anatol, *The Baltic Revolution: Estonia, Latvia and the Path to Independence*, Yale University Press, 1994
40. Lin, Patrick; Abney, Keith; Bekey, George, A., *Robot Ethics: The Ethical and Social Implications of Robotics*, The MIT Press, 2014
41. Melamed, Avi, *Inside the Middle East: Making Sense of the Most Dangerous and Complicated Region on Earth*, Skyhorse, 2016
42. Miller, Christopher, *The War Came To Us: Life and Death in Ukraine*, Bloomsbury Continuum, 2023
43. Mitchell, Melanie, *Artificial Intelligence: A Guide for Thinking Human*. Farrar, Straus and Giroux, 2019
44. Montasari, Reza, *Artificial Intelligence and national Security*, Springer, 2022
45. Murray, Williamson, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, 2012
46. Murray, Williamson; Mansoor, Peter, R., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, 2012
47. Nance, Malcolm, *The Plot to hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election*, Skyhorse, 2016
48. Nasr, Vali, *The Shia Revival: How Conflicts within Islam Will Shape the Future*, W W Norton & Co Inc, 2007

49.Öniş, Ziya; Keyman, Fuat, E., *Turkish Politics in a Changing World: Global Dynamics and Domestic Transformations*, Istanbul Bilgi University Yayinlari, 2007

50.Patrikarakos, David, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century*, Basic Books, 2017

51.Plokhy, Serhii, *The Gates of Europe: A History of Ukraine*, Basic Books, 2017

52.Rid, Thomas, *Active Measures: The Secret History of Disinformation and Political Warfare*, Farrar, Straus and Giroux, 2020

53.Rothbart, Daniel; Korostelina, Karina, K.; Cherkaoui, Mohammed, *Civilians and Modern War: Armed Conflict and the Ideology of Violence (War, Conflict and Ethics*), Routledge, 2012

54.Russell, Stuart, *Human Compatible: Artificial Intelligence and the Problem of Control*, Viking, 2019

55.Scharre, Paul, *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton&Company, 2018

56.Schroeder, Ted, W., *Lethal Autonomous Weapon Systems in Future Conflicts*, Independently published, 2017

57.Sciutto, Jim, *The Shadow War: Inside Russia's and China's Secret Operations to Defeat America*, Harper, 2019

58.Shirreff, Richard, *War with Russia: An Urgent Warning from Senior Military Command*, Quercus, 2016

59.Snyder, Timothy, *The Road to Unfreedom: Russia, Europe, America*, Crown, 2018

60.Stengel, Richard, *Information Wars: How We Lost the Global battle Against Disinformation and What We Can Do About It*, Atlantic Monthly Press, 2019

61.Stryker, Cole, *Hacking the Future: Privacy, Identity, and Anonymity on the Web*, Abrams Press, 2012

62.Weissmann, Mikael; Nilson, Nikolas; Palmertz, Björn; Thunholm, Per, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations,* I. B. Tauris, 2021

63.Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019