Andrea Beccaro[1]

Influence of Emerging Technologies

This chapter aims to better clarify the impact of modern technology on warfare and in particular on the concept of hybrid warfare. To do this, the chapter is divided into three sections in addition to the conclusions. The first part seeks to clarify the impact of modern technology on warfare by briefly examining the terminology used. The second analyses in more detail the relationship between Emerging Disruptive Technologies and the concept of hybrid warfare. The third part is a focus on the current use of drones on modern battlefields. In this way, the paper intends also to clarify a central theme for understanding war, that is, the relationship between it and technology. In the current context, there is no doubt that the cyber environment and the development of AI (Artificial Intelligence) are expanding the range of possible actions in the context of hybrid threats. The development of information technologies from the 1980s has had a huge impact on the development of new operational possibilities. However, we must never forget that war is a political and social phenomenon, and it has a human dimension that cannot be eliminated. From this point of view, technology is exclusively a tool, more or less advanced and more or less effective depending on the contexts and strategies, of a wider and more complex phenomenon.

Technology and war in the 21st century

Multidimensionality. All wars in history have had multiple dimensions and strategic thought itself has always had at least two dimensions (land and sea). Today, however, modern technology has expanded this aspect transforming the concept of multidimensionality into a central term for understanding the conflicts of the 21st century. The concept can be read from two distinct perspectives. On the one hand, the term indicates that modern operations require multidimensional strategies that must include military, political, economic, information and IT tools. On the other hand, multidimensionality refers to the fact that the

[1] University of Turin.

DOI: https://doi.org/10.36250/01237_09

dimensions of strategy have progressively expanded over the last two centuries. Historically, wars have always taken place on the ground and, therefore, land warfare has always been dominant. With the invention of the internal combustion engine, the submarine and the aircraft, new horizons opened up linked to the vertical dimension of the conflict up to the exploration of space and the use of satellites for the collection of information and for communications. Finally, the information revolution has created a "non-space" that has added a further dimension to strategic thought, namely cyberspace. This represents the real revolution in military operations, since the purely military means still used today are often instruments designed and produced decades ago. It is the skills of communication, acquisition of objectives, surveillance and reconnaissance that today have profoundly transformed both those tools and the battlefield. These new technologies have also had a significant impact on training. On the one hand, technological development and the availability of modern individual weapons on the black market has significantly reduced the difference in firepower between a regular soldier of any Western army and that of an irregular fighter. On the other hand, the latter cannot enjoy the advantages of high-level training that derives from the ability to create realistic scenarios within which to test new tactics, weapons or more simply to teach recruits.[2] The cyber aspects are just one of the many facets and various fields of development linked to new technologies that also offer low-cost solutions to small or medium powers as well as to so-called irregular fighters. This creates a strategic situation in which the distinction between regular and irregular is much more blurred and where conflict is fought, even with non-lethal tools, on several different levels.

Ambiguity. Ambiguity indicates duplicity, an ambiguous way of behaving and undoubtedly this is a hallmark of hybrid threats. However, it is certainly not necessary to introduce the term hybrid warfare to understand this aspect because strategy has always been based precisely on the idea of duplicity, of being interpreted in different ways. Luttwak[3] defined this aspect as the paradoxical logic of strategy, namely the fact that in war what appears most logical and simple is probably the worst choice to make precisely because it is the simplest and most obvious option, it is what the enemy is prepared to face. Already Sun Tzu indicated in deception and duplicity one of the distinctive features of military

[2] Boot 2006.

[3] Luttwak 2001.

strategy. For example, in chapter five of *The Art of War*[4] he states that one must give the enemy (the illusion of) a small advantage, so that he will expose himself in the ways we want and then surprise him in a more advantageous context for us. Feints and operations to distract the enemy are central elements to take by surprise in a different sector the enemy who at that point will have positioned his forces and his attention elsewhere. In the 20th century, Liddell Hart[5] with his indirect approach has supported similar ideas precisely with the aim of creating the element of surprise that is the basis of the strategy. Carl von Clausewitz[6] does not directly address the problem but using the terms "fog of war" *(Nebel des Krieges)* and "friction" *(Friktion)* the Prussian underlines how ambiguity pervades all conflicts for the most varied reasons: lack of information, incorrect information, technical problems, human errors, problems relating to the weather or the type of terrain, without forgetting that the actions of the enemy, which we cannot know in advance, constantly modify the environment in which we operate. Therefore, the concept of ambiguity is an element of warfare and strategy that should not surprise. The concept of Gray Zone Warfare[7] is now used to indicate actions of international actors that cannot be identified either as open warfare or as simple peaceful diplomacy actions, they are thus classic ambiguous actions that have the advantage of being easily deniable, but at the same time aim to modify, albeit marginally, to the advantage of those who apply them, the strategic context. But all this constitutes not only the very nature of strategy but also of international politics and diplomacy. Machiavelli spoke clearly of the need to be a fox in politics, emphasising the need to slyly exploit situations and conceal behaviours in order to achieve one's goals. During the Cold War itself, the United States made extensive use of propaganda and hidden or disguised aid such as scholarships, economic aid, etc. to weaken the enemy.[8] What has perhaps changed today is the extent of the ambiguity that derives from the pervasiveness of the media and the Internet. In relation to hybrid threats, one of the major problems is making the political decision-maker understand that certain situations (such as migration or propaganda) can be elements of a broader political conflict strategy.

4 Tzu 1990.
5 Liddell Hart 1991.
6 Clausewitz 1984.
7 Mazarr 2015.
8 Robinson et al. 2018.

Contested Environment. This term encompasses all attempts by an opponent to disturb the United States and its partners in the entire battle space. For example, an opponent could use long-range ballistic and cruise missiles, cyberattacks, and electronic warfare to attack vital elements of the U.S. military structure, including air bases and communications systems.[9] From the end of the Cold War until the beginning of the 21st century, the United States and NATO were used to operating in environments where enemy forces were only partially able to militarily contend the battle space and, consequently, they developed operational capabilities that exploited that particular strategic situation. *Desert Storm* in Iraq in 1991, *Deliberate Force* and *Allied Force* in the Balkans in the 1990s, *Enduring Freedom* in Afghanistan in 2001, *Iraqi Freedom* in Iraq in 2003 were operations in which, albeit with some limitations, the western air forces were able to operate undisturbed. There were minimal casualties, but in general the skies were dominated by western aircraft. Today, this is no longer the case. To better understand this situation, it is necessary to refer to the concept of A2/AD which creates a sort of security bubble in which American aircraft cannot enter (or rather they can but with a high risk) and here a central role is played mainly by missiles of various kinds. The first modern theatre in which the United States has found itself operating in such an environment, with the exception of the Pacific with China which has been implementing this approach for years, is certainly Syria. The aforementioned operations highlight the fact that the contested environment idea is closely related to air operations, which are fundamental for modern military actions, but which are only one of the elements. If we use a land warfare perspective, however, we see how the concept of contested environment is a-historical since land operations have always been contested by an enemy, more or less strong or more or less prepared. Furthermore, modern technologies create a further context space, that of cyber and communication in general. Threats to communications in a contested environment put at risk the entire centralised command and control system that has prevailed in recent decades.[10] Indeed, as the American scholar Stephen Biddle[11] pointed out in a recent volume, in today's battlefields one of the essential requirements for the actors, whether regular or irregular, is to be able to avoid the enemy's firepower for long enough to carry out their political plans. A first way to do so

9 Priebe et al. 2019.
10 Priebe et al. 2019.
11 Biddle 2021.

is that of stealth, that is to hide from the eyes of the enemy in order not to offer a target, and it is certainly the typical approach of irregular warfare. Nonetheless, starting at least from 1914, even the regular forces have increasingly tried to make themselves invisible, since, given the firepower of modern artillery and the increased accuracy of modern weapons, being identified means being hit. Cover and concealment have thus become central elements for modern regular forces. A second way to avoid the enemy's firepower is that of dispersion which also leads to a confusion between the front line and the rear that is typical of the current strategic context. Typically, the irregular fighters disperse over the territory and mix with the civilian population to "disappear" in the eyes of the security forces. However, even the regular armies have abandoned, starting from 1916–1917, the old concepts of formation in line and in mass, introducing, instead, more flexible deployments composed of small units. This has resulted in the progressive dispersion of forces on the battlefield and, therefore, the density of troops on modern battlefields has drastically changed. This trend, on the other hand, did not affect the irregular fighters who historically have always been very dispersed over the battlespace. Consequently, this trend has made the two ways of fighting, the regular and the irregular one, more similar. Since today the density between the two actors on the battlefield is similar and both have a similar firepower, the clear advantage that the regular armies historically had against these actors has progressively been eroded. The technological advantage, which remains on the side of the state actor, is not able to compensate for this levelling of the number of soldiers on the battlefield. As Biddle notes in every war situation in history, be it regular or irregular, the fundamental dynamics of combat is linked to the desire to defend against enemy fire and at the same time to the need to expose oneself in order to use one's firepower. So, lethality and survival are two dynamics always in play and in search of a balance. Greater dispersion in the field also implies greater independence and this implies the need for a more agile and flexible chain of command, in the style of the German *Auftragstaktik*.[12] The exponential increase in the firepower of modern weapons and their accuracy, even the simplest and most common ones readily available on the market for non-state actors, allows a limited number of fighters to be highly deadly and effective.

Information Environment. The term information environment (IE) is new but the concept it describes is not because it defines how information can be

[12] In modern military terminology it can be translated as *Mission Command.*

used to influence the direction and outcome of competition and conflict, or the use of information within the framework of a defined strategy. Any strategic author from Sun Tzu onwards emphasises the important and decisive role of having a superior understanding of one's opponents and the centrality of using that understanding wisely to gain an advantage over them. In short, information is the means by which all the warring parties build mutual understanding of each other and of themselves. Since today we live in a globalised world, the IE of the 21st century is a highly complex "system of systems" on a global level in which information moves and produces consequences with increasing and often high-level and unexpected speed. Such flows are uncontrollable and offer all actors, both state and non-state, important opportunities to develop their influence. In general, IE consists of three dimensions: physical, the environment in which the interaction between geography, infrastructures, individuals, states, cultures, society takes place and where the physical effects occur; virtual, the environment that contains intangible entities; cognitive,[13] afferent to the sphere of perceptions and decisions, constitutes the environment in which the social and psychological effects that influence the behaviour of an individual can be achieved. It is therefore an externally complex and large system impossible to control in its entirety.

Information Manoeuvring (IM). This notion is closely related to the previous one. The concept of manoeuvring is clearly not new since every general in history has manoeuvred, more or less effectively, his army on the battlefield in order to win the clash with the enemy. Certainly, more recent, and from various points of view more nebulous, is the concept of IM and to clarify it we could say that it involves the use of information in all its forms to understand the operating environment better than anyone else and, subsequently, to make the most of this advantage. The goal of IM is to model perceptions to ensure that the activities and intentions of the army are adequately recognised by allies, populations and adversaries. IM requires a large degree of integration and is intrinsically linked with capabilities in the cyber, space, maritime and air domains. It, therefore, brings together the forces that work in the cyber field, electronic warfare, surveillance, reconnaissance, counterespionage and influence activities (psychological warfare) to achieve the desired effect. It is a concept that fits well into the notion of Gray Zone Warfare and useful for countering some hybrid threats.

[13] Jervis 1976.

Emerging and Disruptive Technologies (EDT) and NATO

NATO defines emerging and disruptive technologies (EDT) technologies such as artificial intelligence (AI), autonomous systems, advanced manufacturing, biotechnologies and quantum technologies. Emerging and Disruptive Technologies (EDT) is a notion that highlights the role of modern (and future) technology in the conflicts of the 21st century. There is no doubt that today we are facing a time of profound and rapid changes in technological terms, but great caution is needed in assessing their impact on the international context in general and on future conflicts in particular. First, if we look at the history of war only very few technologies have radically reshaped the dynamics of international conflicts. In fact, most technological innovations have led to incremental advances over a medium to a long period of time. Furthermore, some of those advances have completely disappeared despite having prompted great promise. For example, the introduction of chemical weapons was widely interpreted as a radical change in the way of waging war. Yet, that type of weapons, although repeatedly used even in more recent times, proved to be impractical, easier than expected to counter and less effective than other conventional explosives in inflicting damage and countering enemy operations. Other technologies, on the other hand, became crucial in warfare only after major advances in other areas allowed them to reach their full potential. This is the case, for example, of drones, since unmanned aircraft were already present in the middle of the twentieth century, but it is only with modern information technologies that they could become an essential military tool. This means that even when war technologies have a real and significant impact on the conduct of warfare, it can take decades to be effective in military terms because that technology not only needs to be refined, but also needs to be placed in a suitable strategic and doctrinal context. Secondly, even if today's emerging technologies were ready to introduce major changes in the international system, it would be very likely that they could have contradictory effects, since technologies can be both destabilising (opening unprecedented scenarios for new or old actors, the best recent example is Turkey that using its drones has been able to increase its military and diplomatic leverage in the MENA region) and stabilising (creating equality between previously opposed actors). Nor should it be forgotten that it is probable that other factors may intervene to mediate the effects of new technologies on the international system: geography, the distribution of power, military strategy, domestic and organisational policies

and social and cultural variables. As Sechser, Narang and Talmadge note,[14] it is difficult to predict the impact of new technologies because the directions they can take are very different and even contradictory. While some modern technologies are easy to access even for non-state actors with limited resources, as far as EDTs are concerned, they are technologies that require large investments, a good industrial base and time, consequently they remain available to a few actors, namely the United States, China and to some extent Russia. A fundamental problem for understanding EDTs is the fact that they are inherently Dual Use, so the progress made in this area can be (also) destined for civil use and in the same way investments in the civil sector can open up new possibilities in the military field. However, this does not mean inertia since it is now possible to study and examine the EDT sectors on which we must concentrate to understand how these technologies can influence conflicts and international politics. This is what NATO has tried to do in the last years. In London, in December 2019, NATO leaders agreed on a roadmap for the implementation of EDT-related measures. The final document highlights the breadth and scope of new technologies to maintain the technological advantage that NATO has always had over its enemies. Then the document encourages to continue and to increase the resilience of critical infrastructures and energy security (the reference is clearly to Russia). Particular emphasis was given to the security of communications with reference to 5G and the need to exclude possible adversaries (the reference is clearly to China), recognising the need to rely on secure and resilient systems, i.e. on ones managed by allies. Another important aspect is space, an operational domain for NATO, which therefore aims to defend it. At the same time, the pervasiveness of cyberattacks and therefore the need to strengthen the capacity to discourage and defend against this kind of threats is underlined.[15] In February 2021, NATO defence ministers approved an EDT strategy to develop a specific Alliance policy response. In the following March, the NATO Advisory Group on Emerging and Disruptive Technologies published its first annual report[16] which identifies the areas that the Alliance must consider in the context of the new technological landscape. The final document underlines how EDTs are developing at a particularly fast pace and this forces NATO to do the same if it does not want to be overtaken

[14] Sechser et al. 2019.
[15] NATO 2019.
[16] NATO 2020a.

by potential adversaries. To this end, the experts highlighted the need for greater and more integrated cooperation between the Alliance, its members and both the private and public research sectors (universities in particular). Moreover, the working group identified five scientific areas of particular interest:

- First, the key technology sectors: artificial intelligence; quantum computing as well as quantum cryptographic systems and the development of quantum-scale material; data security and therefore algorithms and systems to protect communications and transactions; developments in miniaturisation, energy harvesting and energy storage; the design, synthesis and manipulation of materials at the atomic–molecular level or bioengineering and chemical engineering.
- Second, the socio-technical context, where information systems directly influence change in the physical world and evolve autonomously through detection and data. Here, advances in autonomy, the ubiquity of high-speed communications and other similar advances will rapidly stimulate human–machine interaction.
- Third, the struggle for resources such as water, food, energy and raw materials will continue to grow and intensify. The struggle for data as a resource will be added and this will create new, or reinforce existing, asymmetries on a global level.
- Fourth, space will be the key theatre of the future within which NATO must guide the development of a technologically advanced, complex and articulated environment. The organisation will have to develop internal skills in innovative technologies and innovation and actively participate in the development of new discoveries in order to optimally exploit the brightest minds in industry, government and academia.

What therefore emerges from the document and from the recommendations of the experts is the need for NATO to become an organisation capable of adapting and adopting new technologies at an adequate pace to the technological landscape linked to EDTs. This transformation can only happen if technological literacy is expanded throughout the organisation, an efficient network of Innovation Centres is established, drawing on NATO's existing innovation capabilities, funded projects in this direction and established partnerships with industry and academia. However, in line with some of the recommendations of the NATO Advisory Group on Emerging and Disruptive Technologies at the

Brussels summit of 2021, the NATO 2030[17] agenda was approved with which NATO wanted to launch a new initiative regarding civil–military defence, the Defense Innovation Accelerator for the North Atlantic (DIANA) with the aim of strengthening transatlantic cooperation on critical technologies, promoting greater interoperability and exploiting civil innovation through collaboration with academia and the private sector. In Brussels in 2021, it was also decided to create a fund to finance activities in the EDT sector and in NATO innovation. The fund will invest in start-ups working on EDT and dual technologies in areas critical to the security of the Allies. In particular, the Alliance has identified seven key areas: artificial intelligence (AI), data and information technology, autonomy, quantum technologies, biotechnologies, hypersonic technologies and space.[18] It should not be forgotten that these research sectors must be inserted in a broader technological context of which the four main characteristics that will profoundly influence the future developments of military technology must be pointed out: the characteristic of being intelligent or integrated with AI to create "intelligent" applications technology; be interconnected by exploiting the network and networks of sensors, organisations, individuals and autonomous agents, connected through new encryption methods; be distributed thanks to the possibility of decentralised and ubiquitous storage and computing; and be digital by digitally mixing the human, physical and informational domains. Even more recently, NATO[19] published its strategy regarding AI. The theme is absolutely central both because AI is the technological aspect that can implement all the others and because together with cyber it has the potential to open scenarios that are currently difficult to evaluate. The final document, among other things, highlights some core tasks and sectors related to AI, including: accelerating and integrating the adoption of AI into existing capabilities, improving interoperability; protect and monitor our technologies; identify and safeguard against threats arising from the use of AI by state and non-state actors. Professor Ralph Thiele, expert on hybrid threats with leading publications on the subject and researcher at Hybrid CoE in Helsinki, highlighted some salient points regarding this aspect and specifically highlighted three technologies that will be central:

17 NATO 2021a.
18 NATO 2020b.
19 NATO 2021b.

- First, AI plays a leading role as an engine and multiplier for other technologies and development sectors. Its particular potential lies in the analysis of large amounts of data, in the optimisation of processes, support for decision-making processes and the development of an inter-divisional organisation for understanding situations. However, since AI is currently still a vulnerable technology, it must be handled with caution.
- Second, autonomous systems such as artificial intelligence, machine learning and big data rely primarily on software. The most significant development in this field is undoubtedly that of drones. With the development of technology and greater integration capacity in the not-too-distant future entire swarms of intelligent systems will work together: drones, jets, ships and other interconnected systems. The concepts of human–machine teamwork shape this process. Unmanned Autonomous Systems act, individually or in swarms, as part of a team in close collaboration with human decision makers. While machines take on boring and dangerous operational tasks, humans focus on cognitive aspects and leadership functions, because autonomous systems lack the flexibility of human intelligence.
- Third, quantum science promises to be the driving force of the next revolution. New IT architectures allow the processing and analysis of big data, leading to better search algorithms and faster calculations. A significant consequence in this field is the fact that quantum computers would be able to penetrate the cryptography that states, banks and other actors use to protect their secrets. An important military application for a functional quantum computer is the ability to hack encrypted military servers and servers of an opponent's national infrastructure systems almost instantly.[20]

Drones in contemporary battlefields

One of the most clear and excellent examples of how modern technology is used on the battlefield is related to the use of drones. We have already discussed in one of the previous chapters of this book *(Different Regional Theatres),* how hybrid groups, such as ISIS, have used such weapon during the fight improving both their military and intelligence gathering capabilities. The brief section is to take into account different case studies that highlight the role of both state

[20] Thiele 2021.

and non-state actors in using this modern technology. It is important to note that although we are used to see drones supporting military operations during land actions, they are used in all military domains, land, sea and air and by both state and non-state actors. An example of this has been the attack on 29 July 2021, when three armed "suicide drones" attacked the *Mercer Street,* an Israeli-managed commercial oil tanker. Two drones missed the tanker during an attempted first strike, but one successfully flew into the *Mercer Street*'s bridge during a second strike.[21] The attack killed a British security guard and the vessel's Romanian captain. Despite the fact that no one claimed responsibility for the attack, experts and analyst said that the available evidence points to Iran. Therefore, this operation was just one of the last actions of a U.S.–Iran "shadow war" that has been simmering across the Middle East for the past years. While it is uncertain who deployed the drones (Iranian regional proxies? Or elements of the Iranian armed forces?), it is well known that Iran has become what we can call a "drone superpower". From strikes on the government-owned Saudi Aramco facilities in eastern Saudi Arabia in September 2019 to attacks on U.S. troops in northern Iraq in July 2021, a string of drone strikes ties back to Iran. Moreover, Iran started to use drones in 1984 when Iran's Islamic Revolutionary Guard Corps (IRGC) formed its first unmanned aerial vehicle (UAV) unit. More recently, Israel's defence minister, Benny Gantz, accused Iran of providing foreign militias from Yemen, Iraq, Syria and Lebanon with drone training at an airbase near the city of Isfahan.[22] However, Iran is not the only actor in the Middle East to use drones and the increasing presence of this war tool in the region is one of the most important and relevant elements of contemporary security and a very concerning tactical development. Research[23] has recorded 440 drone attacks conducted by militants through 2020. Over 98% of them have occurred in the Middle East mainly from two groups, the Islamic State and Houthi rebels in Yemen, responsible for over 80% of these. Another research has found that militant groups use drones especially for disrupting opponent command and logistics and delaying the movement of military personnel and materiel. They do not use drones for what we may call "strategic bombing", i.e. for targeting military centres of gravity,[24] even though defining what is a "centre

21 The Times of Israel 2021.
22 Middle East Eye 2021.
23 Haugstvedt–Jacobsen 2020.
24 Doctor–Walsh 2021.

of gravity" is a controversial and thorny issue. Summarising the different use of drones by militias in the Middle East, it is possible to list at least three main uses. First, drones, commercial or military ones, are used to support ground operations and the best-known example is ISIS during the battles to defend cities in Iraq and Syria. Second, drones, commercial or military ones, are used to attack logistic hubs, arms depots, critical infrastructure and command headquarters behind front lines. This kind of attack is probably the most common one. The attack against the *Mercer Street* is of this type, but the attacks that Shia militias carried out in Iraq against U.S. troops and bases can also be listed in this category. Although a database of these attacks does not exist, it is possible to say that U.S. troops, bases and facilities (including the U.S. embassy in Baghdad) have been targeted around 60 times between the summer of 2020 and the summer of 2021. It is true that none of these attacks have resulted in fatalities or critical damage, but they did prompt the Biden Administration to order retaliatory airstrikes against the militant groups behind them. Probably the most serious attacks were conducted against airports both in Baghdad and in Erbil, which was targeted at least two times: on 25 July 2021, a drone attack targeted a base near al-Harir, northeast of Erbil; and on 11 September 2021, Erbil International Airport has been targeted by two armed drones. Moreover, at the end of August 2021, eight people were injured in a drone attack on Saudi Arabia's Abha airport. The drone was intercepted and shrapnel hit the runway. It was the second attack on the airport in 24 hours, when a ballistic missile struck the airfield.[25] Two elements of the use of drones in Iraq are relevant and concerning. First, the Iraqi PMF (Popular Mobilization Forces), mostly Shia militias, are supported by Iran and it is known that they used military Chinese drones CH-4B, but also the Iranian drone Mohajer-6s. During a military parade in late June a Mohajer-6 was seen armed with two small munitions similar to the Ghaem series.[26] Second, during the recent Israel–Gaza conflict, it has been claimed that some of the drones flying over Israel had been sent from Iraq or Syria. Iraqi pro-Iran militias, many of them present in Syria as well, continuously threaten that they can attack Israel from Iraq. There was information in February 2021 that drones were launched from the Iraq – Saudi Arabia border toward a royal palace in Riyadh. This fact shows that pro-Iran armed groups in Iraq have chosen this new vehicle, which ensures greater camouflage and target accuracy and greater

[25] Al-Monitor 2021.

[26] Mitzer–Oliemans 2021.

protection for their operations.[27] Moreover, from April 2018 to October 2019, the Houthis executed 115 drone attacks, of these, 62 were conducted against civilian airports or critical infrastructure.[28] The third use of drones is less known because it rarely grabs the headlines but it is very important for the militias in order to improve their military capacities. Several militant groups have used unarmed drones for intelligence, surveillance and reconnaissance operations. Drone-based intelligence, surveillance and reconnaissance offers significant value to militants for relatively little cost or risk. ISIS is again a good example. It used these kinds of drones to re-direct in real time suicide vehicles (SVBIEDs) during the battle of Mosul in order to bypass Iraqi defences and find new ways to approach the designed targets. More recently, it has been reported that the Islamic State's affiliate in West Africa has used drones to place under surveillance the locations and movement of counterinsurgent forces in northeast Nigeria.[29] Since this constant, extensive and widespread use of drones, what is surprising is that such militias have never used the drones to carry out terrorist attacks, even though drones seem particularly well-suited to such a task. The flying drones are not the only threat that comes from unmanned vehicles in the Middle East. In fact, since 2017, Houthi forces in Yemen have been perfecting their use of maritime drones to carry out attacks against maritime vessels and port facilities in the region. As the flying drones, also these attacks have not yet resulted in several fatalities or critical damage but have caused material damage to a number of ships and led to the temporary shutdown of one of Saudi Arabia's port. Moreover, as to the flying drones, the majority of all Houthi maritime drone attacks were directed not against military targets but instead against commercial and civilian ones: four targeted civilian ports and two targeted oil production and distribution facilities.[30] This brief section has showed the considerable and substantial impact of drones used by irregular militias in the Middle East. This is an increasing threat because current technology offers different tools and possibilities that irregular groups can use in the future to improve their military capabilities. We are witnessing a profound technological revolution that, in contrast to what we experienced, for example during the Cold war, is an open one. That means that each group, or even person, can use modern technologies, improve them, combine different tools and

27 Saadoun 2021.
28 Weiss 2019.
29 Foucher 2020.
30 Haugstvedt 2021.

create something new and unexpected. A similar phenomenon occurred, for instance, in the 19th century with the invention and the development of dynamite.[31] Therefore, it is important to analyse current operations in order to understand beforehand possible evolution and novelties.

Conclusion

The focus of this chapter on technology must not make us forget that war is an extremely complex and articulated socio-political phenomenon that cannot be understood solely and exclusively through a purely technological interpretation. However, even when speaking of technology, not all analysts agree in outlining which is the best way to implement modern and advanced technologies. From this point of view, a recent article[32] highlights some limitations of modern strategic thought focused on technology. In fact, the two authors, experts on issues related to cyber threats, underline how the same capabilities, which led the United States to exploit the information revolution (the so-called RMA) to their advantage and that made them in the two decades after the end of the Cold War a power superior to all others, have now become troubling vulnerabilities. The U.S. now carries out campaigns that depend heavily on the digital operations so much that they are vulnerable to new cyber threats, but those same campaigns are not yet sufficiently advanced to be able to take advantage of the latest information technologies. The aforementioned NATO documents answer this problem by saying that we need to increase our efforts and further improve our technologies. The authors support a very different thesis that is more in line with the hybrid threats approach because they invite to review old concepts and find a new approach whose objectives must no longer be speed and decision-making advantage, but on the contrary persistence and resilience. The focus should therefore be on building decentralised networks, investing in tactics that decrease the economic cost of warfare, and developing weapon systems and tactics that do not stop working suddenly and catastrophically, but gradually lose their capabilities in a while once hit. The problem that the authors highlighted is not so much related to technological advancement and, therefore, to the fact that other international actors develop more advanced technologies,

[31] Cronin 2019.

[32] Schneider–MacDonald 2020.

but the fact that the threats against modern information technology adapt faster than the information revolution on which Western strategic thought in recent decades has been based. Modern systems are indeed very vulnerable to network failures and data manipulation. Since the beginning of the computer revolution, its supporters have argued that the victory was the result of a greater knowledge on the local situation which would consequently have allowed greater accuracy of the strikes, while increasing both the speed of action and the distance between target and launch platform. Consequently, investments in technology favoured efficiency and speed over safety and resilience and the acquisition of a small number of expensive and elaborate weapon systems (a clear example of this is the endless controversy related to the F-35).[33] On the contrary, today we should invest in resilience and in systems that change the cost equation by favouring quantity over quality and decentralisation over speed. The old networks were, and remain, strongly centralised, today they would be more secure and resilient networks with high density, small nodes and multiple paths. Such networks are less vulnerable to attack and create less of a cascade effect when compromised with single nodes that can continue to operate. In addition, this race towards the latest technological advance has indeed led to some tactical advantages related to the use of highly technological tools, but at the same time has created a great strategic cost problem. The example of the Hamas missiles that nearly ran out of Israel's expensive Iron Dome in May 2021 is just one of many examples that can be given. It would, therefore, be smarter today to invest in cheap products and disposable technology in order to create mass and resilience. It is, therefore, necessary to combine the modern, advanced and expensive (and thus scarce and difficult to replace) weapon systems with cheaper autonomous sensors and platforms designed to create friction and slow down the opponent's action. Another problem created by the digital revolution is the enormous mass of information. At the beginning, many argued that this was good as it would allow detailed knowledge and greater precision. However, today we know that, while not denying those advantages, the flow of information can be transformed into a weapon both to confuse the enemy (the theme of ambiguity returns) and to undermine it internally through propaganda or fake news. In this context, we no longer need more technology, more AI, more information, but men and soldiers able to interpret, understand, reason and, therefore, able to contextualise what they read from the information.

[33] O'Malley–Hill 2015.

Questions

1. Can you describe the use of drones in the Middle East region?
2. How does NATO approach the problem of Emerging Disruptive Technologies?
3. What is ambiguity?
4. What is contested environment?

References

Al-Monitor (2021): Drone Attack on Saudi Airport Injures 8. *Al-Monitor,* August 2021. Online: https://www.al-monitor.com/originals/2021/08/drone-attack-saudi-airport-injures-8

Biddle, Stephen (2021): *Nonstate Warfare. The Military Methods of Guerillas, Warlords and Militias.* Princeton: Princeton University Press.

Boot, Max (2006): *War Made New. Weapons, Warriors, and the Making of the Modern World.* New York: Gotham Books.

Clausewitz, Carl von (1984): *On War.* Princeton: Princeton University Press.

Cronin, Audrey K. (2019): *Power to the People. How Open Technological Innovation is Arming Tomorrow's Terrorists.* Oxford – New York: Oxford University Press.

Doctor, Austin C. – Walsh, James I. (2021): The Coercive Logic of Militant Drone Use. *Parameters,* 51(2), 73–84. Online: http://doi.org/10.55540/0031-1723.3069

Foucher, Vincent (2020): The Islamic State Franchises in Africa: Lessons from Lake Chad. *International Crisis Group,* 29 October 2020. Online: https://www.crisisgroup.org/africa/west-africa/nigeria/islamic-state-franchises-africa-lessons-lake-chad

Haugstvedt, Håvard (2021): Red Sea Drones: How to Counter Houthi Maritime Tactics. *War on the Rocks,* 3 September 2021. Online: https://warontherocks.com/2021/09/red-sea-drones-how-to-counter-houthi-maritime-tactics/

Haugstvedt, Håvard – Jacobsen, Jan Otto (2020): Taking Fourth-Generation Warfare to the Skies? An Empirical Exploration of Non-State Actors' Use of Weaponised Unmanned Aerial Vehicles (UAVs–'Drones'). *Perspectives on Terrorism,* 14(5), 26–40.

Jervis, Robert (1976): *Perception and Misperception in International Politics.* Princeton: Princeton University Press.

Liddell Hart, Basil (1991): *Strategy.* New York: Meridian.

Luttwak, Edward (2001): *Strategia. La logica della guerra e della pace.* Milano: Rizzoli.

Mazarr, Michael J. (2015): *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Carlisle: The United States Army War College Press.

Middle East Eye (2021): Israel's Gantz Says Iran Giving Militias Drone Training Near Isfahan. *Middle East Eye,* 13 September 2021. Online: https://www.middleeasteye.net/news/israel-iran-gantz-militias-drone-training-isfahan

Mitzer, Stijn – Oliemans, Joost (2021): The Militiamen's UCAV: Mohajer-6s in Iraq. *Oryx,* 31 August 2021. Online: https://www.oryxspioenkop.com/2021/08/the-militiamens-ucav-mohajer-6s-in-iraq.html

NATO (2019): *London Declaration.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London on 3–4 December 2019. Online: https://www.nato.int/cps/en/natohq/official_texts_171584.htm

NATO (2020a): *NATO Advisory Group on Emerging and Disruptive Technologies. Annual Report 2020.* Online: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf

NATO (2020b): *NATO, Science and Technology Trends 2020–2040.* Online: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

NATO (2021a): *NATO 2030.* Online: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf

NATO (2021b): *Summary of the NATO Artificial Intelligence Strategy.* Online: https://www.nato.int/cps/en/natohq/official_texts_187617.htm?fbclid=IwAR235gFvoqQuyr-B1iC5EcBSholcs2Anl9Le6O7LRjC7wDJuuHu1BSjh1eI

O'Malley, Derek – Hill, Andrew (2015): Close Air Support in 2030: Moving Beyond the A-10/F-35 Debate. *War on the Rocks,* 28 May 2015. Online: https://warontherocks.com/2015/05/the-a-10-the-f-35-and-the-future-of-close-air-support-part-ii/

Priebe, Miranda – Vick, Alan J. – Heim, Jacob L. – Smith, Meagan L. (2019): *Distributed Operations in a Contested Environment. Implications for USAF Force Presentation.* Santa Monica: Rand.

Robinson, Linda L. – Helmus, Todd C. – Cohen, Raphael S. – Nader, Alireza – Radin, Andrew – Magnuson, Madeline – Migacheva, Katya (2018): *Modern Political Warfare. Current Practices and Possible Responses.* Santa Monica: Rand.

Saadoun, Mustafa (2021): Iraqi Armed Factions Using Drones against US-led Coalition. *Al-Monitor,* May 2021. Online: https://www.al-monitor.com/originals/2021/05/iraqi-armed-factions-using-drones-against-us-led-coalition

Schneider, Jacquelyn – MacDonald, Julia (2021): The Information Technology Counter-Revolution: Cheap, Disposable, and Decentralized. *War on the Rocks,* 19

July 2021. Online: https://warontherocks.com/2021/07/the-information-technology-counter-revolution-cheap-disposable-and-decentralized/

Sechser, Todd – Narang, Neil – Talmadge, Caitlin (2019): Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War. *Journal of Strategic Studies,* 42(6), 727–735. Online: http://doi.org/10.1080/01402390.2019.1626725

The Times of Israel (2021): Multiple Iranian Drones Used in Deadly Attack on Israeli-Operated Ship – Report. *The Times of Israel,* 31 July 2021. Online: https://www.timesofisrael.com/multiple-iranian-drones-used-in-deadly-attack-on-israeli-operated-ship-report/

Thiele, Ralph ed. (2021): *Hybrid Warfare. Future and Technologies.* Wiesbaden: Springer. Online: http://doi.org/10.1007/978-3-658-35109-0

Tzu, Sun (1990): *L'arte della guerra.* Roma: Ubaldini Editore.

Weiss, Caleb (2019): Analysis: Houthi drone strikes in Saudi Arabia and Yemen. *FDD's Long War Journal,* 7 August 2019. Online: https://www.longwarjournal.org/archives/2019/08/analysis-houthi-drone-strikes-in-saudi-arabia-and-yemen.php