Nicola Cristadoro[1]

Ideologies and Motivations

Nowadays, does it still make sense to speak of armies in the traditional sense, intended as military forces of large numerical entity for land use in large-scale war operations? Considering the 'special military operation' carried out by Russia with the full-scale invasion of Ukraine on 24 February 2022, the answer would appear to be affirmative. However, if we consider most conflicts that have erupted or protracted over the past decade, this conception appears at least anachronistic. Observing the use of the land forces of the nations fighting in the various contemporary operational theatres, we do not see divisions, brigades or regiments that manoeuvre facing each other for the conquest and occupation of a territory or for its defence. If the Kurdish Peshmerga still wear uniforms and fight in regular units that, despite internal divisions, make them comparable to an army, the same cannot be said of their direct enemies, the Islamic State of Iraq and Syria (ISIS) fighters. These, in fact, despite being largely veterans of the Iraqi army after its disbandment, incorporate foreign fighters from different areas of the world and fight with a mixture of weapon systems and multiform technical-tactical procedures, according to the canons of 'asymmetric warfare'.

Examples worldwide

The concept of 'asymmetric warfare' itself, at present, appears outdated. If the Warsaw Pact and NATO doctrines for conventional warfare belong to prehistory, 'asymmetric warfare' can now be considered history. Asymmetrical were the conflicts of decolonisation in Africa, the Viet Cong campaigns in Indochina, the actions of Palestinian terrorist organisations against the Israeli security forces, the attacks of the Taliban and Al Qaeda-affiliated against the coalition deployed in Afghanistan. To refer to contemporary conflicts, it seems more appropriate to speak of 'ambiguous', 'non-linear' and 'hybrid' warfare, i.e. wars fought at different levels and prevailing over the ways in which the opposing forces clash on the ground. The term 'hybrid warfare' currently refers with

[1] University of Turin.

DOI: https://doi.org/10.36250/01195_05

immediacy to Russia. This term was coined in 2002 by William J. Nemeth (for more details see the chapter authored by Eado Hecht in this book) to describe the Chechen insurgency, which saw the fusion, hence the adjective 'hybrid', of guerrilla techniques with modern military tactics, resorting extensively to the support of civilian technology from mobile phones to the Internet. The social paradigm presented by Nemeth, which sees the degeneration of an evolved society into a 'hybrid society' as a premise for the development of 'hybrid' conflicts, is interesting. "There is increasingly a body of work that is challenging the accepted norm of peaceful pre-state societies that turned violent only as higher and more centralized forms of societal organization became prevalent […]. Devolving societies are societies that are returning to more traditional forms of organization, but are doing so unevenly. That is, these societies are bringing with them an eclectic mix of modern technology as well as political and religious theory and institutions as they devolve […]. These societies, many of which retain the trappings of the state system, are either a multitude of warring clans contained within the previous state boundaries, or a mostly homogenous socio-political unit that is fighting against a perceived oppressor. In either case these hybrid societies are a mixture of the modern and the traditional. Hybrid societies in turn have organized hybrid military forces, and it is these forces that will challenge military and diplomatic planners in the future. Currently a large body of work exists regarding hybrid military forces under the rubric of Fourth Generation Warfare, New Warfare, or more conventional terms such as Low Intensity Conflict and Terrorism. Fourth Generation Warfare coined by Bill Lind and others in the late 1980's saw warfare in non-states as developing along a divergent path when compared to that being developed by Western nations. The developed world is increasingly moving toward "Advanced Technology" warfare, which will embed the increasing reliance on high technology seen Western society in Western military forces. Countering this in non-western states, and especially hybrid societies, is an increasing shift toward an idea driven concept of war. This idea driven concept of war […] envisions a mix of terrorism and Low Intensity Conflict that is non-national or transnational in nature and bypasses the western military to directly attack western cultural."[2] The illegal annexation of Crimea to Russian territory and the contribution to instability in the eastern provinces of Ukraine, notably the Donbas, by the Russian Federation and its armed forces have provided a significant example of 'hybrid warfare',

[2] Nemeth 2002: 2–3.

both at the tactical and strategic-operational levels, even ahead of the full-scale invasion in February 2022. Russian actions in Ukraine and Crimea appear clearly in line with this conception, although many scholars of military history and doctrine have pointed out that such an operational choice is nothing new for Russia. An example, albeit a prototypical one, of the adoption of this tactical conception is represented by *Operation Storm 333* conducted in Afghanistan on 27 December 1979 for the capture of President Hafizullah Amin's residence and his elimination by KGB special forces, in conjunction with Army and GRU units. In order to deceive the enemy and take them by surprise, the Soviet soldiers engaged in this operation did not wear the uniforms and insignia of their own units, but Afghan uniforms, except for a white armband tied to one arm, to recognise each other. What we can otherwise call 'ambiguous warfare' involves elements with a very high training and disciplinary profile who, without wearing a uniform and bearing distinctive symbols, are placed in combat zones in a very short time and, in collaboration with local supporters, on the sidelines of traditional operations resort to psychological operations, intimidation and bribery to undermine the adversary's resistance. By 'ambiguous warfare' one can also indicate a certain *modus operandi* in conducting warfare, which was in use in U.S. governmental circles between the 1960s and 1980s and is still widely practised today in both the Iraqi and Syrian scenarios. The *Phoenix Program* implemented between 1967 and 1975 in Vietnam under CIA supervision is indicative of such procedures. Through infiltration, capture, terrorism, torture and assassination, the aim was to identify and 'neutralise' the structure of the National Liberation Front of South Vietnam, the paramilitary organisation better known as the Viet Cong. Even more significant is the support given to the paramilitary units of the Contras in Nicaragua in the late 1970s, which today serve as a model for similar organisations such as the Death Squads active in Iraq or the Free Syrian Army (FSA) operating in Syria. In general, the definition prefigures situations in which a belligerent state or non-state entity deploys military and paramilitary units in a confusing and deceptive manner to achieve military and political objectives, disguising the direct participation of its armed forces in operations. Complicating the model is the attempt to describe modes of operation that fall below the threshold of conventional military conflict. There are in fact, especially in Russian military philosophy, two sub-categories that need to be explored in depth. The 'grey zone warfare' on the one hand and 'hybrid warfare' on the other. In particular, the latter "is more limited to the battlefield, whereas Grey Zone Warfare also considers the political sphere and the

international framework, with all the possibilities for action that these allow […]. It involves even less military action than hybrid warfare […]. Its three main characteristics are ambiguity, a low degree of distinctiveness and the possibility of denying everything".[3] Hence, the topicality of the thought of General Valeriy Gerasimov, the Russian Chief of Defence Staff, who goes beyond the 'asymmetrical' model by elaborating a doctrine that envisages attacking the adversary economically, cognitively and physically by making extensive use of unconventional procedures. In particular, in the perspective of deploying forces capable of operating on a post-modern battlefield, it is preferable to replace traditional manoeuvre and logistic support units with small units that are flexible in terms of deployment, extremely mobile, fast in action and, perhaps, without insignia and badges that can be traced back to their affiliation and nationality. We speak, of course, of Special Forces. The reference to the figures of the American and Soviet 'military advisers' active in Latin America, Asia and Africa between the 1960s and 1980s is immediate. If this aspect already constitutes a peculiar element of the 'ambiguous warfare', such a definition becomes more comprehensible if one considers the other actors that make up the military structure in today's theatres of war, such as Libya, Syria, Iraq, Afghanistan and, extremely representative, Ukraine, with the events in Crimea and the Donbas region. In fact, alongside Special Forces from countries other than the areas of operation and interested in controlling the policies and resources of these areas, there are local paramilitary groups, mercenaries, groups of civilians loyal to one or the other party on an ethnic basis and, last but not least, criminal organisations interested in profiting from the trafficking linked to the conflict. In this already sufficiently confused picture, one must not overlook the increasingly cogent role of hackers, the 'lords of cyberwar' who, with their skills and increasingly sophisticated tools at their disposal, represent the vanguard of the 'infowar'. To them belongs the domination of 'white', 'grey' or 'black' propaganda, and theirs is the ability to strike devastatingly at the nerve centres of a state's economy, society and politics, by compromising or neutralising computer networks. It will be increasingly difficult to determine 'who is who', and this premise portends a further evolution of future war into a form of uncontrollable conflict that we would call the "total chaos warfare". It is difficult for a culture such as that of the West, which, at least in theory, is based on principles of transparency and democracy, or which, *a priori,* repudiates war of aggression in its constitutional dictates, to conceive

[3] Ottaviani 2022: 33.

of such an approach to warfare. Above all, it is difficult to win against adversaries who base their tactics on such doctrinal principles. To understand, therefore, who engages in this type of operation and for what purpose, we are helped by the concept of 'sharp power', which we can metaphorically refer to as a sharp knife that pierces, penetrates or perforates the media and political environment in the targeted countries. "Today's authoritarian states – notably including China and Russia – are using "sharp power" to project their influence internationally, with the objectives of limiting free expression, spreading confusion, and distorting the political environment within democracies. Sharp power is an approach to international affairs that typically involves efforts at censorship or the use of manipulation to sap the integrity of independent institutions. This approach takes advantage of the asymmetry between free and unfree systems, allowing authoritarian regimes both to limit free expression and to distort political environments in democracies while simultaneously shielding their own domestic public spaces from democratic appeals coming from abroad."[4] However, as we shall see, Russia and China are not the only states that are extremely proactive in the conduct of undeclared or even denied wars. We opened with one question and two others emerge as a premise for the development of this discussion. What are the motivations that lead a state to choose to engage in a hybrid conflict and what forms of government best favour the planning, organisation and conduct of an undeclared war? In the following we will examine several state and non-state realities that seem to us to represent suitable models for answering the questions formulated.

Russian establishment

Following the collapse of the Soviet Union in 1991, Russia struggled to find and reclaim its place in the world order. Reactionary elements within the government, intelligence services and armed forces found common cause with the new economic elites and elements of the Russian Orthodox Church in their desire to reclaim the loss of empire. Thus, even before the *de jure* dissolution of the Union of Soviet Socialist Republics (USSR), Moscow began to reassert its control over the members of the Commonwealth of Independent States (CIS). Russian methods of intervention evolved from conflict to conflict as leaders sought the most

[4] Walker 2018: 9–23.

efficient ways to bring weaker powers to their knees while avoiding the stigma of imperialism, invasion and war with the West.[5] The events that led to Lithuania's independence in 1991 were the first lesson learned about exercising power abroad in the post-Cold War era. Large-scale conventional operations against sovereign states would expose the Kremlin to unwanted scrutiny by the International Community (IC), international pressure and protests within Russia itself. To maintain control over the 'near-abroad' states, Moscow would have had to exercise power in a more clandestine and concealable manner. The most effective tactics implemented by Russia to act in the so-called 'grey zone' are (dis)information operations and cyber operations, followed by political coercion and space operations. The Russian info-ops of the Internet Research Agency – whose owner Yevgeny Prigozhin is also the financier of the Private Military Company 'Wagner' – continue to be generously funded, relentless and prolific. The coercive activity directed at the socio-political structures in Europe has become increasingly aggressive over time, following Putin's attempts to block NATO's eastward expansion. In this context, Moscow's deeper ties with Serbia, with the Bosnian Serb component and the failed covert operation to block the Prespa Agreement,[6] must be read with growing concern. Even in space, Russia has demonstrated its capacity and unscrupulousness in targeting states from which it feels threatened, with actions to jam GPS signals during NATO military exercises, with attacks against U.S. commercial and allied military satellites, and even by damaging the sensors of a Japanese satellite with lasers.[7] The prerogative offered by hybrid warfare, especially acting in what we have called the 'grey zone', is precisely that of dereliction of responsibility for its own actions, and during the campaigns in Ukraine, wherever possible, Moscow strenuously denied its involvement, exploiting elements of proximity and resorting to deception to evade the IC's condemnations associated with a conventional armed invasion.[8] The Federal Security Service (FSB) and the Ministry of Internal Affairs (MVD), in fact, assumed the role of directing forces acting by proxy, an organisational technique that began at the end of the last century and would

5 Herd–Akerman 2002: 357–372.

6 The "Prespa Agreement" is an agreement reached in 2018 between Greece and the Republic of Macedonia, under the auspices of the United Nations, resolving a long-standing dispute between the two. Apart from resolving the terminological differences, the agreement also covers areas of cooperation between the two countries to establish a strategic partnership between them.

7 Harrison et al. 2019.

8 The United States Army Special Operations Command 2015.

continue in subsequent Kremlin-led war operations. Let us recall that from 1999 to 2009, Moscow directed a campaign that effectively suppressed the Islamic insurgency in Chechnya and reasserted Russian control of the region. As long as wars could technically be considered internal affairs, Russia was able to avoid accusations of aggression. However, global outrage in the wake of civilian deaths and the growing refugee problem led Putin's military and intelligence components to transfer control of counterinsurgency operations to reliable proxies such as local militias and paramilitary forces to be deployed in place of regular Russian troops. In developing their operations, therefore, the Russians alternately denied involvement or downplayed the size and activities of their forces. In particular, they introduced the use of information warfare on an unprecedented scale. In the 2008 Russian–Georgian conflict, for instance, Russian agents extensively used cyberwar and intense propaganda to neutralise the Georgians' combat options and smear them in the press as aggressors, even accusing them of genocide. The Russian military brought journalists to the area of operations to reinforce Russia's message of protecting the population from Georgian aggression. Moscow carefully managed television broadcasts both at home and in the region, highlighting the atrocities the Georgians allegedly inflicted on the people of South Ossetia. These procedures have been named 'spetzpropaganda' and are taught at the Department of Military Information and Foreign Languages of the Ministry of Defence Military University. As an academic discipline, it is aimed at military personnel, intelligence officers, journalists and diplomats. The doctrine specifies that an information campaign is multidisciplinary and includes politics, economics, social dynamics, military, intelligence, diplomacy, psychological operations, communications, education and cyber warfare. In general, Russian information warfare aims to influence the consciousness of the masses, both at home and abroad, to condition it with a view to a clash of civilisations between Russian and Western Eurasian culture. Through the coordinated manipulation of the entire information domain including newspapers, television, internet websites, blogs and other media, Russian operatives attempt to create a virtual reality in the conflict zone that influences perceptions or replaces the truth with versions that fit the Russian narrative.[9] In Crimea and the subsequent operations in the Donbas, Russian 'spetzpropaganda' developed the theme that pro-Russian intervention was necessary to save the Ukrainian people from submission to the Kiev regime imposed "by the Banderovtsy and the Maidan

[9] Darczewska 2014.

fascists".[10] This is the background to the strategic thinking of General Valery Gerasimov,[11] Chief of the Defence Staff of the Russian Federation. General Gerasimov's main thesis is that modern conflict differs significantly from the paradigm of World War Two and even from the Cold War conflict. Instead of declared wars, strict definition of military and non-military efforts, and large conventional forces to be deployed in battle, the modern conflict features undeclared wars, hybrid operations combining military and non-military activities, and the employment of smaller forces with specific training: *spetsnaz,* paramilitaries, mercenaries. Gerasimov explained that the 'coloured revolutions' and the 'Arab Spring' have shown that the line between war and peace is blurred. Although liberal democratic uprisings may not look like war, they often result in foreign intervention (both overt and clandestine), chaos, humanitarian disasters and civil war. These activities can become the typical war of the modern era and Russian military practices must evolve to adapt to the new methods. Modern warfare, said Gerasimov, focuses on intelligence and the domination of the information space. Information technologies have reduced the spatial, temporal and information gap between army and government. Targets are achieved in remote contactless warfare; the strategic, operational and tactical levels, as well as offensive and defensive actions, have become less distinguishable. Asymmetric actions against enemy forces are more common. The military dimension, therefore, must include information warfare. Armed, but not in uniform, Russian forces in Crimea have provided Moscow with the possibility of deniability, albeit implausible. The pro-Western press called the intruders 'little green men', while Russian cultural supremacist theorist Aleksandr Dugin called them 'nice men', referring to their kindness and diplomatic retreat once an area was secured. The goal is the very essence of Sun Tzu's expressed ideal of "winning without fighting". In Crimea, it worked. In eastern Ukraine, it did not and led to an escalation of the conflict. To catalyse domestic consensus, the Putin Administration went so far as to popularise the idea of a NATO plan to invade Russia and even foreshadowed that the West, led by the U.S., intended to annex Crimea. Sevastopol would then become a NATO naval base. Linked to these themes, it then played on the idea that the Russian people, with its history of religious, cultural and military greatness, had been artificially divided after the collapse of the Soviet Union. Once again, the West was presented as

[10] The United States Army Special Operations Command 2015.

[11] Cristadoro 2022.

the architect of the conspiracy to prevent Russia from enjoying unity, peace, security and its rightful place in the world order. From the Russian point of view, since the West is persecuting Russia, everything becomes permissible in the pursuit of a true justice that reaffirms Moscow's deprived role. Let us come to the events of 24 February 2022. The invasion implemented with the massive recourse to conventional forces lends itself to a twofold interpretation: on the one hand, it may represent the failure of the Russian infowar in Eastern Ukraine, hinting at an extreme attempt by Putin to make up for the failures of the policy of deploying 'asymmetrical' forces in the Donbas; on the other hand, in perfect adherence to the 'Gerasimov Doctrine', it represents the logical continuation of the Russian info campaign, which is partly designed to establish the conditions for invasion, should it be necessary.

Dragon on the attack

China aggressively and effectively employs many hybrid 'grey zone' tactics. The main ones are provocation using forces under state control, economic coercion, cyber operations and space operations. The motivations behind Beijing's warfare through 'grey zone' tools, and the tools themselves, are summarised in NATO's Strategic Concept 2022. "The People's Republic of China's (PRC) stated ambitions and coercive policies challenge our interests, security and values. The PRC employs a broad range of political, economic and military tools to increase its global footprint and project power, while remaining opaque about its strategy, intentions and military build-up. The PRC's malicious hybrid and cyber operations and its confrontational rhetoric and disinformation target Allies and harm Alliance security. The PRC seeks to control key technological and industrial sectors, critical infrastructure, and strategic materials and supply chains. It uses its economic leverage to create strategic dependencies and enhance its influence. It strives to subvert the rules-based international order, including in the space, cyber and maritime domains. The deepening strategic partnership between the People's Republic of China and the Russian Federation and their mutually reinforcing attempts to undercut the rules-based international order run counter to our values and interests."[12] A peculiar element of Beijing's operations in the 'grey zone' is the construction of artificial islands. Indeed, since 2013, China has

[12] *NATO 2022 Strategic Concept:* 5.

engaged in dredging and building islets in the Spratly Islands archipelago and constructing outposts throughout the Paracel Islands. To enforce these activities, the Chinese rely on both the coast guard and the People's Armed Forces Maritime Militia (PAFMM).[13] Interestingly, members of this militia operate in the South China Sea without identification marks and are therefore referred to as 'little blue men'. The reference to their counterparts who participated in the 2014 invasion of Crimea is obvious. At least as far as the Spratly Islands are concerned, China has turned some islands into military bases, "complete with radar domes, shelters for surface-to-air missiles and a runway long enough for fighter jets."[14] According to Admiral Philip S. Davidson, this militarisation of the area indicates that "China is now capable of controlling the South China Sea in all scenarios short of war with the United States".[15] Let us now look at economic coercion; this includes the Belt and Road Initiative (BRI) economic and foreign policy project. Although the BRI improves Chinese trade links and reduces China's domestic industrial production surplus, Beijing uses its economic leverage to influence the interests of other states[16] and for the purpose to "deter confrontation or criticism of China's approach to or stance on sensitive issues".[17] It must also be considered that the BRI's 'debt-trap diplomacy' creates opportunities for China to introduce military forces in states where local development interventions are carried out, as in the case of Djibouti, where the naval base established by Beijing is of strategic importance both militarily and economically for controlling trade routes. Nevertheless, alongside the development of the BRI there has been the Digital Silk Road (DSR) initiative to bring technological advances and digital infrastructure to developing economies. Like the BRI, the DSR can create economic benefits for China, but there are well-founded concerns that the initiative has unstated security purposes.[18] For example, through the installation of fibre-optic cables, Chinese state-owned or state-affiliated enterprises can acquire large amounts of data that the Chinese Government could eventually use to exert pressure in areas outside of the economy.[19] In the race for 5G, it is feared that once a company like Huawei has installed its network, it will be used for espionage

13 Thomas 2020.
14 Beech 2018.
15 Beech 2018.
16 Cristadoro 2021.
17 Department of Defense 2018: 12.
18 Department of Defense 2018.
19 Harding 2019.

activities,[20] aimed at acquiring sensitive data useful for industrial purposes, but also for potential coercive influence. Economic coercion aimed at acquiring intellectual property or conducting industrial espionage is carried out through cyber espionage or by Chinese companies under the control of Guoanbu, the foreign intelligence agency. Such activity includes the acquisition of "companies and technology based on their government's interests – not on commercial objectives".[21] For example, from 2013 to 2016, Chinese companies sought to acquire several businesses in the semiconductor industry. China's potential dominance of that industry could play a crucial role in altering the future global military balance, as semiconductors are essential in the components of advanced military systems.[22] China, therefore, relies on cyber operations in the 'grey zone' that go beyond purely economic purposes. Cyberwar is a favoured route to conduct espionage and intelligence gathering, but also to target the critical infrastructure of other states and interfere in political processes abroad. Let us not forget that the cyber activities conducted by Russia are also paradigmatic in this respect. Lastly, considering Space as a new warfighting domain, China's conspicuously funded space programme is aimed at developing a range of activities in the 'grey zone'.[23] China continues to develop a range of space interdiction capabilities designed to limit or prevent an adversary's use of space assets during crises or conflicts. The People's Liberation Army has historically managed China's space programme and continues to invest in improving China's capabilities in space Intelligence, Surveillance, Reconnaissance, satellite communications, satellite navigation and meteorology, as well as human spaceflight and robot space exploration.[24] China utilises its orbital and terrestrial resources to achieve its civil, economic, political and military goals and objectives. People's Liberation Army (PLA) strategists consider the ability to use space systems and to deny their use to adversaries as strengths in the conception of modern, computerised warfare, and therefore, the Chinese Armed Forces are pursuing a programme to strengthen its military space capabilities, in contradiction to the government's statement against the militarisation of space. Space operations are likely to be an integral component of other PLA campaigns and will play a key role in enabling

[20] Cristadoro 2021.
[21] Cooper 2018.
[22] Cooper 2018.
[23] Harrison et al. 2019.
[24] Office of the Secretary of Defense 2017.

suitable actions to counter third-party intervention during military conflicts. In addition to the research and possible development of satellite jammers and directed energy weapons, China has likely made progress on kinetic energy weapons, including the anti-satellite missile system tested in July 2014.[25] Beijing is conducting increasingly sophisticated satellite operations and is likely experimenting with dual-use technologies for use in orbit that could be applied to space interdiction missions. The PLA's Strategic Support Forces, established in December 2015, play a leading role in managing Chinese aerospace warfare capabilities.[26] Commercial satellite imagery has shown Chinese military grade jamming equipment deployed on islands in the South China Sea, which can be used to interfere with communications, Positioning, Navigation and Timing (PNT) signals or any other satellites in the region.[27] China has also been involved in using its cyber capabilities to target space systems. Importantly, although China is the state with the greatest capacity to exploit the "grey zone", it has chosen not to intervene indiscriminately in all areas. This apparent restraint requires further reflection on whether China feels inhibited by U.S. actions or is simply self-regulating for other reasons. If the latter is true, these reasons can be identified and understood and could offer several elements to dissuade China from applying its tactics in the "grey zone" in the future.

Hezbollah and Tehran

Iran's support to proxy groups acting in Lebanon, Syria, Iraq and Yemen is one of its most effective tools to achieve its national interests by fighting in the 'grey zone'. The Islamic Revolutionary Guards Corps (IRGC), the notorious Pasdaran, is the paramilitary organisation executing Iranian proxy policies, with close ties to groups such as Hezbollah in Lebanon, the Houthis in Yemen, the National Defence Force Militia in Syria and the Badr Corps in Iraq, among others.[28] Drawing on its special forces unit known as the Quds Force, the IRGC is able to train and advise its auxiliary forces – estimated at 250,000 fighters – and thus poses a significant threat to Tehran's adversaries in much of the Middle East.

25 Office of the Secretary of Defense 2017.
26 Office of the Secretary of Defense 2017.
27 Gordon–Page 2018.
28 McInniss 2017: 25–33.

The Quds Force was established in the early 1990s to enable the ayatollahs' regime to operate covertly outside Iranian borders. The goal was to build an operational mechanism that would take the Islamic Revolution out of Iran.[29] As part of its ongoing struggle against Israel, Iran's strategy uses proxy organisations for two main reasons. Firstly, because of the considerable distance between Israel and Iran. The more than one thousand kilometres separating the two states constitute an objective operational difficulty for Iran for a direct attack on Israeli territory. Secondly, Iran is very concerned about the Israeli response, should it directly attack Israel. Therefore, the use of proxy organisations negates the difficulties related to the distance between Iran and Israel, effectively engaging the latter on two fronts of struggle, one in the north against Hezbollah in Lebanon and the other in the south against Hamas and Islamic Jihad in the Gaza Strip. This strategy also allows Iran not to be directly involved in the confrontation with Israel.[30] To achieve this goal, Tehran continues to support paramilitary formations under its control in Lebanon and the Gaza Strip and to supply them with various weapons systems, including rockets and missiles.[31] According to Israeli military intelligence, the precision missile programme was designed for two purposes. The first was to reduce the range of fire towards Israel. While, as mentioned, the distance between Iran and Israel is thousands of kilometres, southern Lebanon is only a few hundred kilometres from the nerve centre of the State of Israel in Tel Aviv and Gush Dan. Therefore, while Iran would need to launch long-range missiles to hit Israel, Hezbollah can achieve the same goal from Lebanon with short-range rockets. The second purpose is to move the battlefield away from Iran. Since firing at Israel from Syria and Lebanon may foresee a logical Israeli retaliation against these countries rather than Iran, Tehran is better off financing its proxy organisations and arms supplies, thus avoiding putting itself at risk in the front line of its policy of aggression against the Jewish state. The best-known paramilitary organisation is Hezbollah, which began its military operations following the expulsion of Palestine Liberation Organisation (PLO) forces from Lebanon in 1982 during the First Lebanon War. Inspired by the religious justification of leading Shi'a ideologues such as Ayatollah Khomeini, remember the suicide bombings against Israeli, American and French targets located in Lebanon. Hezbollah succeeded in advancing the status of the

[29] Katz–Hendel 2011.
[30] Eilam 2019.
[31] Bergman 2018.

Shi'a community in Lebanon from a persecuted and deprived community to the most powerful and dominant community in the country, while repressing the Christian community in Lebanon. The Iranians, who have sought to propagate the religious principles that guided the Islamic revolution and improve the quality of life of Lebanese Shi'as, have poured hundreds of millions of dollars into supporting Hezbollah. Thus, Iran has founded many social institutions for the Shi'a in Lebanon, such as hospitals, clinics, universities, cultural institutions, and radio and television stations.[32] In parallel, it has trained and armed Hezbollah members into a military militia serving the IRGC.[33] The organisation has about 20,000 men in readiness, of which 5,000 are elite fighters and between 20,000 and 50,000 are reserve fighters.[34] Hezbollah bases its defence on the civilian population of the area in which it operates. Although Iran's theocratic conception is as far removed from Chinese state atheism as possible, there is an affinity with Mao Zedong's principle of "mingling with the population like fish in the sea" and gaining their consent. In terms of technical-tactical procedures (TTPs), the organisation establishes its headquarters on the lower floors of ten-storey residential buildings and also in residential buildings where it hides weapons such as missiles and rockets.[35] Hezbollah thus exercises a form of deterrence against possible Israeli attacks, which would be subject to harsh criticism by the IC for the 'collateral effects' of such a decision. Hezbollah, however, has also been criticised for its tactical-strategic choice. In response to the criticism, the organisation stated that, considering the weakness of the Lebanese army, it is the only one that can guarantee a buffer between Israel and Lebanon to protect the latter from any Israeli aggression.[36] Although Hezbollah started out as a typical militia to be employed in asymmetric warfare tactics, over time it has evolved into an organisation capable of fighting different types of war. During the Lebanese civil war, when it was but one of many militia groups in the country, Hezbollah mainly launched suicide bombings and frontal attacks on Western and Israeli forces, both methods that, militarily, are neither sophisticated nor efficient. Hezbollah's quiet evolution from a guerrilla force to a military structure capable of applying more conventional TTPs went unnoticed

[32] Harel–Issacharoff 2008.
[33] Katz–Hendel 2011.
[34] Eilam 2016.
[35] Kaunert–Wertman 2020: 99–114.
[36] Harel–Issacharoff 2008.

and only became evident during the 34-day-war against Israel in 2006. The organisation displayed tactics and capabilities far beyond what was expected, to be fully framed in the typology of hybrid warfare. After the Israeli invasion, Hezbollah took full advantage of Lebanon's rocky terrain, ideal for ground movements but impractical for armoured manoeuvres. It has focused its battle-positions on easily defensible hilltop villages, which offer excellent observation and firing ranges and are inhabited by populations sympathetic to its cause. Despite being outnumbered, its units proved to be cohesive, well-trained, disciplined and experienced in how to control territory. Equipped with an effective chain of command and control, thanks to a complex communication system, Hezbollah successfully employed hedgehog defence tactics, creating strongholds in fortified bunkers, like a regular force. During the conflict, it continued to fire rockets at Israel using concealed launchers, even behind enemy lines. None of these tactics are characteristic of guerrilla forces, which usually rely on population-centred methods of concealment. In essence, Hezbollah took Israel by surprise because it acted in a manner that is not really attributable to an irregular fighter, nor to the regular army of a State. In the conduct of Iran's hybrid warfare, cyberattacks and info-ops are also increasing rapidly, as more and more Iranian hackers work to target individuals, companies and government entities around the world, focusing mainly on the Middle East region such as Saudi Arabia and Israel. In particular, Iran carried out a data deletion attack on dozens of Saudi government and private networks between 2016 and 2017.[37] The regime in Tehran exercises tight control over the domestic dissemination of information, restricting television broadcasts, social media use and internet access, which greatly limits foreign influence and promotes pro-regime narratives.[38] Internationally, info-ops have helped Iran perpetuate its image as a regional power, particularly as a challenger to Saudi Arabia and Israel, while simultaneously presenting itself as a reliable international partner. Iran's info-ops also include space as an arena of the 'grey zone'. Indeed, Tehran has on several occasions blocked satellite communication transmissions, as in the case of the interruptions of Voice of America and BBC broadcasts.[39]

[37] Coats 2019.
[38] Eisenstadt 2017: 62–72.
[39] Hicks – Hunt Friend 2019.

Kim against Seoul and Washington

North Korea's main activities in the 'grey zone' include cyber operations, political coercion and military provocations. North Korea has a skilled and sophisticated cyber force capable of carrying out disruptive operations around the world.[40] Notable cyber operations attributed to North Korea include the 2014 attack on Sony, the 2016 cyber heist against the Bangladesh Bank, and the 'WannaCry' malware worm released in 2017.[41] North Korea's political coercion aims to strengthen the regime's position by exploiting U.S. efforts to coordinate with its allies and regional partners.[42] For example, the ongoing trade war between the United States and China has forced the Trump Administration to seek a compromise between engaging in the maximum pressure campaign against Pyongyang and efforts to conclude a credible pact with Beijing on tariffs.[43] The trade war has unintentionally strengthened North Korea's political position by pushing U.S. regional allies, mainly South Korea and Japan, further into China's regional economic sphere of influence. According to Bloomberg columnist Daniel Moss: "The trade war could have been an opportunity to drive a wedge between China and its regional trading partners […]. Yet the Trump administration's irreverence for the collateral damage of its actions might end up drawing China's neighbours closer into its orbit."[44] The South Korean Government's announcement of the launch of an $8 million food aid package for North Korea, a decision supported by President Trump, is one such example of Kim's astute ability to amass a relative political advantage without comparable benefits for Washington and its regional allies.[45] As Brookings expert Jung Pak wrote in 2018: "At a minimum, North Korea is attempting to sow division within South Korea and shape Seoul's policies toward ones that are favourable to Pyongyang."[46] Regarding military provocations, it is sufficient to consider that the North Korean Army has deployed 70% of its forces within 60 miles of the Korean Demilitarised Zone (DMZ). The tactics developed by North Korea in the 'grey zone' also manifest themselves in space, considering that the country is probably the most active satellite system jammer in the world.

40 Chanlett-Avery et al. 2017.
41 Chanlett-Avery et al. 2017.
42 Pak 2018.
43 Bradsher – Sang-hun 2019.
44 Moss 2019.
45 Sang-hun 2019.
46 Pak 2018.

North Korea regularly blocks GPS signals in South Korea, jamming air routes and harbours close to the DMZ.[47] Fundamental, however, is the strategy adopted by Pyongyang through the constant threat aimed at neighbouring 'enemy' countries through missile tests and the proclamation of readiness to use the nuclear weapon.[48] In this, moreover, the North Koreans are on the same line as Russia's current cross-domain coercion strategies. For instance, the Democratic People's Republic of Korea's (DPRK's) short-range ballistic missile (SRBM) tests carried out on 4 May 2019 and 9 May 2019 highlighted the lack of cohesion in the alliance opposing Pyongyang,[49] as well as creating rifts within the U.S. Government itself.[50] Nevertheless, the U.S. was already engaged in coordinating a multinational 'maximum pressure' campaign aimed at deterring North Korea's future nuclear development, bringing the regime's leaders to the negotiating table, and ultimately denuclearising the Korean peninsula.[51] For the foreseeable future, two aspects are likely to influence the U.S. response to North Korean 'grey zone' activities. First, diplomatic grievances between North Korean and U.S. officials threaten to prolong stalled negotiations. The outcomes of talks in Hanoi in 2019 between former President Trump and North Korean leader Kim Jong-un bear witness to this. The second concerns the U.S. – South Korea joint military exercises. According to political analysts, a downsizing of the joint exercises would benefit the strategic objectives of North Korea, Russia and China at the expense of effective multilateral coordination between the U.S., South Korea and Japan. "Any such drawdown would face strong pushback from Congress and Japan, whose conservative government is deeply wary of North Korea's intentions."[52] North Korea's behaviour after the Hanoi summit also suggests that Kim is determined to find 'a new way' to strengthen his international position in the absence of an agreement with the U.S. To this end, Kim's visit to Russia in April 2019 and his continued engagement in China to receive economic support can be interpreted as a strategy to divide the U.S. and its regional allies while finding ways to circumvent international sanctions.[53] Russian investments in North Korea's infrastructure and mineral resources, for example, would strengthen

47 Harrison et al. 2019.
48 ANSA 2022.
49 Denyer–Joo 2019.
50 Sanger et al. 2019.
51 Cha – Fraser Katz 2018: 87–100.
52 The Japan Times 2019.
53 Min-hyung 2019; Herskovitz–Li 2019.

Kim's strategic position by reducing his dependence on a U.S.-brokered deal.[54] Essentially, North Korea's 'grey zone' activities are likely to exploit any glimmer of ambiguity that the U.S. would allow in its regional commitments.

Hamas's Asymmetrical Warfare

Hamas, an acronym of Ḥarakat al-Muqāwama al-Islāmiyya (Islamic Resistance Movement), born at the time of the first Intifada as the Palestinian operational arm of the Jamaʿat al-Iḫwān al-muslimīn (Muslim Brotherhood), has today become the hegemonic Palestinian organisation in the Gaza Strip. From the territories of the Strip it has been waging a war of attrition against Israel for years, consisting of suicide bombings, rocket attacks, incendiary balloons, and infiltration into Israeli territory through tunnels. The EU, the USA and several other states consider Hamas a terrorist organisation, Russia, Turkey, Iran and Qatar diverge from this position. The U.K. only considers the Izz al-Din al-Qassam Brigades, the military wing of Hamas, to be a terrorist organisation. By contrasting guided missiles and drones, hence Israeli technological superiority, with the narrative of the young Palestinian fighter armed with a sling and stones, i.e. the rhetoric of the First Intifada, Hamas puts itself on an asymmetrical war footing and, in terms of communication, in an advantageous position. We are in fact witnessing the reversal of a founding myth of Israel, namely the myth of David against Goliath. The organisation, however, is the author of precisely 'hybrid' actions, as emerges from a deliberately contradictory narrative. The one that places the stone-throwing boy alongside the Izz al-Din al-Qassam brigades' demonstrations of military might, in which Quassam rockets make a fine show. Hamas has an interest in showing itself weak, but also strong, and if then, such a strategy is accompanied by an effective use of the new technologies such as the social networks, the capacity to determine the flows of strategic communication ends up becoming even more incisive and viral. Here, then, is the effectiveness of the image of what appears to be little more than a child, targeting a Merkava tank with a stone throw. The image could be recent or old, it could have been taken in Gaza as in the West Bank, it could even be the result of a skilful photomontage. It does not matter. The point is that it is a recurring image, used by the mainstream media, along with hundreds of other very similar ones, to depict short news reports on events that

[54] Isachenkov 2019.

have been going on since 1948. So what is so special about it? It is simply viral. Viral because it is aimed at left-wing Israelis' sensitiveness and because it does so by evoking the myth of David versus Goliath, overturning it. In a nutshell, it colonises the collective imagination. We can imagine looking for Hamas's model of strategic-communicative rationality, confirming, albeit updating them to the times of social communication, the dynamics of guerrilla warfare and Arab revolt already in use in Lawrence of Arabia's time, i.e. asymmetrical warfare practices, a war fought with armed clashes (Bedouin guerrilla warfare against regular Ottoman troops), but also of semiotic clashes (Lawrence dressed in Arab clothes entering Cairo and announcing to General Allenby the taking of Aqaba), a war therefore to all intents and purposes asymmetrical, made up of weapons and signs (a *semio-war*).[55] It is at this point that the cross-media use of the different platforms available to Hamas intervenes, the social ones such as Facebook, Twitter, the YouTube channel, but also the radio Al Quds and the TV Al Aqsa. The latter two media with signal transmission capacity also in Israel, which become *echo chambers*[56] in which the final addressee receives, among the many, the only informative and media fragments "that confirm the ideological positions already acquired and on which he surrounds himself and feeds".[57] When effective, Hamas propaganda is believed not so much because of the truth or verisimilitude of the message itself, but because it is directed towards a category of receivers – those on the other side of the channel – who already know or suspect those things. Let us now look at the effectiveness of the info-ops carried out using 'human shields'. On 23 August, the Israel Defense Forces (IDF) bombed a residential building (Al Zafer tower), believed to be used as Hamas headquarters, causing its collapse. This incident also provoked international condemnation of Israel, thanks in part to Hamas's communicative ability to accuse Israel of war crimes. What remains is the message that Israel strikes civilian targets, causing innocent deaths and committing war crimes. Exactly the effect desired by Hamas. In the analysis in question, the use and results obtained by Hamas in the use of human shields is emphasised, a fact consistently applied to the following areas:

[55] Fabbri–Montanari 2004: 1–27.
[56] Quattrociocchi–Vicini 2016.
[57] Marino–Thibault 2016: 25–26.

- Placement of rocket launcher, artillery and mortar positions near densely populated areas, often near buildings protected by the Geneva Convention (schools, hospitals or mosques).
- Placement of military infrastructure, command centres, critical infrastructure, weapons depots, close to or near civilian areas or major road junctions.
- Protection of terrorist cells, safe havens or men injured or in danger because they are threatened by targeted killings by the IDF, near civilian, residential or commercial areas.
- Use of civilians, in the event of conflict in the strip, for intelligence tasks. Such reckless use of civilians means that Hamas can play the game with the IDF in a scenario where Hamas always wins. If the use of Israeli military force produces an exponential increase in civilian casualties, Hamas can move the propaganda machine by activating the combined use of social media, TV and independent journalists, having a good game in using the weapon of lawfare to accuse Israel of war crimes against innocent civilians. Otherwise, if Israel depletes its strike force so as not to hit innocent civilians, limiting the strikes as much as possible, Hamas has gained 'reflexive control' (Gerasimov *docet!*).

The practice of using human shields is not something Hamas is at pains to deny. At a press conference in 2018, Khaled Meshaal, the movement's political leader at the time, uttered the following words: "If you [Israelis] are so crazy as to decide to enter Gaza, we will fight you. You will face not only hundreds of fighters, but also one and a half million people, driven by the desire to become martyrs."[58] Another indicative confirmation of this orientation comes from a sentence uttered by Hamas spokesman Mushir Al-Masri in 2006, when the IDF warned of its intention to strike the home of one of the organisation's leaders, Waal Rajub Al-Shakra's in Beit Lahiya.[59] The Hamas spokesman pronounced the following words: "The citizens will continue to defend their pride and their homes, acting as human shields, until the enemy withdraws."[60] Finally, the statement by another Hamas spokesperson, Sami al-Zuhari, dating back to July 2014, thus pronounced in the hottest weeks of the Israeli invasion, is also interesting: "The fact that the

[58] Conference Press 2018.
[59] Al-Aqsa TV 2006.
[60] Al-Aqsa TV 2014.

population is happy to sacrifice themselves against the Israeli planes with the aim of protecting their homes, proves the validity of this strategy. Hamas therefore calls on our people to apply this practice."[61] The strategic communication model adopted by Hamas, largely like that of Hezbollah, is a multivariate model, based on a plurality of supporting media, both traditional and non-traditional, and is aimed both at 'friends', internally such as the Palestinian humma and Arab and Persian sympathisers, and at enemies, mainly Israel and the U.S. If in the past it was the traditional television medium that dominated such as Al Aqsa TV and Al Quds Radio, it was gradually joined by the YouTube medium and then the social networks, where trolls and memes, truth, fake news and misinformation began to work, mainly targeting the public opinions of Western countries and the Arab world, as well as the Israeli pacifist left-wing components. In such a model, dissemination strategies are typically mixed media that represent the coordinated use of several social media, or cross-media focused on a specific channel, e.g. Al Aqsa TV, the primary driver of the communication strategy and social as a means of disseminating the information produced by the primary channel. How can Israel counter these actions? It is clear that the repeated attacks against Al Aqsa TV[62] or Al Quds Radio[63] are not only useless, but even harmful. The message that immediately rebounds is that Israel strikes civilians and silences the media to cover it up. Inevitably, because of these critical issues, one wonders whether Israel has a counter-propaganda system capable of withstanding these new challenges, a system as efficient as its military one. For instance, it would be interesting to investigate, but this inevitably represents a new research question, whether Israel is capable of infiltrating Hamas chats by effectively counterpunching trolling practices, instead of scrambling in a futile and wasteful attempt to dismantle misinformation and virality with philological debunking. On the other hand, traditional military manuals have for decades admitted that guerrilla warfare is answered not by traditional methods, but by counter-insurgency warfare. This learning also applies to the infosphere in which pitting troll against troll is clearly not enough, and where it is necessary to dust off old, tried and tested weapons,

[61] Al-Aqsa TV 2014.

[62] Hit both in 2008 and July 2014, during the 2014 Israel–Gaza conflict by Israeli air strikes that also affected the radio station. In 2014, the TV station continued to broadcast, while the radio station went silent, only to return to the airwaves.

[63] Currently, a powerful antenna provided by Hezbollah re-transmits Radio Al Quds broadcasts from Lebanon into Israeli territory. The Shin Bet alleges that the radio transmissions contain encrypted messages addressed to Hamas fighters infiltrated in East Jerusalem and the West Bank.

such as the 'semiological guerrilla warfare' theorised by Umberto Eco, who stated that "the battle for the survival of man as a responsible being in the Age of Communication is not won where communication starts, but where it arrives".[64] It is interesting to note that, except for Hamas, which represents a non-state entity, all the other situations examined relate to states that have in common that they are not governed by democratic governments. This peculiarity is what allows them to resort so indiscriminately and invasively to hybrid warfare, or at least to act unscrupulously in the 'grey zone'. It is precisely autocratic, theocratic or dictatorial self-referentiality, depending on the nuance that sets the stage for governments themselves to self-justify their aggressive policies towards other states perceived as a threat to their own interests. It is also true that the U.S., the great theorists of these doctrines of contemporary warfare, has also long been engaged in activities that to all intents and purposes prefigure hybrid modes and 'grey' operations in its conduct of foreign policy. In the democratic world, however, they are the exception and not the rule and act by virtue of their superpower role. All other countries in the democratic area that find themselves embroiled in the 'total chaos warfare' taking place on the globe, act according to defensive principles and modes, not offensive ones like those of the various autocracies. Even Israel, for decades engaged in a struggle for its own survival, operates in adherence to defensive and containment strategies. We mentioned the United States as a superpower; American governments have always justified their courses of action by presenting themselves as bearers of the values of freedom and democracy. In truth, even the United States absolutely tends to look after its own interests like almost everyone else, but Washington needs a theoretical framework that gives moral dignity to its behaviour. Actually, it has to be said that there are peoples and cultures that traditionally care little for freedom and democracy; on the contrary, they judge them to be 'disvalues'. We conclude with a reflection that on the surface it has nothing to do with what is discussed in this essay, but only on the surface. The United States is also the home of rock'n'roll, and Western culture is where such music took root and grew. We think back with regret to the words of *Wind of Change* by Scorpions: "Blows straight into the face of time/Like a storm wind that will ring the freedom bell/For peace of mind/ Let your balalaika sing/What my guitar wants to say." How many expectations betrayed and how many dreams of universal peace shattered! True, I recognise

[64] Eco 2021.

that even in the West, there is a lot of rubbish being passed off as music, but unlike in the countries that are the subject of this study, at least here one can choose what to listen to and play.

Conclusion

'Ambiguous war', 'non-linear', 'hybrid', 'grey' war – different ways of referring to wars fought in ways that are now increasingly distancing themselves from traditional conflict concepts and doctrines, both at the strategic and tactical levels. Non-conventional warfare assumes a dominant role and, therefore, the military component in contemporary conflicts often does not wear a uniform or display distinctive symbols. In general, contemporary wars prefigure situations in which a belligerent state or non-state entity deploys military and paramilitary units in a confused and deceptive manner in order to achieve military and political objectives, concealing the direct participation of its armed forces in operations. Alongside combat forces, whether regular or irregular, we find forms of combat ranging from cyber warfare to information warfare, from the unscrupulous use of diplomacy to economic warfare. The United States are the major theorists of this type of conflict, but Russia, China, Iran, North Korea, as well as non-state entities such as Hamas, are the nations that on the world geostrategic scenario for the past twenty years have implemented hybrid combat, in fact triggering real conflicts that, with different forms and modalities, have manifested themselves in different parts of the planet. We are talking about countries where the concept of democracy and human rights is non-existent; it is significant that in a world where war, at least in principle, is repudiated as an instrument for resolving political disputes (let us recall von Clausewitz's definition of it), there are nations that, lacking the humanitarian scruples that are the patrimony of Western culture founded on Law, have found a pragmatic solution to conduct operations that until the recent past would have been openly indicated as full-fledged war actions.

Questions

1. In which forms can the asymmetrical dimension of hybrid warfare evolve as an instrument of struggle by organisations that do not have regular armed forces?

2. Is it likely that negotiation and its procedures themselves become a combat mode of hybrid warfare, depending on the messages they communicate?
3. Can hybrid warfare turn into a form of "total chaos warfare" due to the complexity, variety and quantity of interests and actors involved?

References

ANSA (2022): Corea del Nord, Kim: deterrenza nucleare contro Seul e gli Usa. *ANSA,* 28 July 2022. Online: www.ansa.it/sito/notizie/topnews/2022/07/28/corea-del-nord-kim-deterrenza-nucleare-contro-seul-e-gli-usa_baa60dd8-3b9d-4e52-8709-52f94e6b1a7a.html

Banasik, Mirosław (2015): How to understand the Hybrid War. *Securitologia,* 1, 19–34.

Beech, Hannah (2018): China's Sea Control Is a Done Deal, "Short of War With the U.S.". *The New York Times,* 20 September 2018. Online: www.nytimes.com/2018/09/20/world/asia/south-china-sea-navy.html

Bergman, Ronen (2018): *Rise and Kill First. The Secret Story of Israel's Targeted Assassinations.* New York: Random House.

Bradsher, Keith – Sang-hun, Choe (2019): With Kim's Visit, China Shows US It Has Leverage on Trade. *The New York Times,* 08 January 2019. Online: www.nytimes.com/2019/01/08/business/china-north-korea-kim-trade.html

Cha, Viktor – Fraser Katz, Katrin (2018): The Right Way to Coerce North Korea: Ending the Threat Without Going to War. *Foreign Affairs,* 97(3), 87–100.

Chanlett-Avery, Emma – Rosen, Liana W. – Rollins, John W. – Theohary, Catherine A. (2017): *North Korean Cyber Capabilities: In Brief.* Congressional Research Service. Online: https://sgp.fas.org/crs/row/R44912.pdf

Coats, Daniel R. (2019): *2019 Worldwide Threat Assessment of the US Intelligence Community.* Office of the Director of National Intelligence. Online: www.dni.gov/files/ODNI/documents/2019-ATA-SFR—-SSCI.pdf

Cooper, Zack (2018): *Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare.* Foundation for Defense of Democracies. Online: www.fdd.org/analysis/2018/09/05/understanding-the-chinese-communist-partys-approach-to-cyber-enabled-economic-warfare/

Cristadoro, Nicola (2021): *La mossa del Drago. Strategia politico-militare e guerra di intelligence nella Cina del XXI secolo.* Torino: Edizioni Il Maglio.

Cristadoro, Nicola (2022): *La Dottrina Gerasimov. La filosofia della guerra non convenzionale nella strategia russa contemporanea.* Torino: Edizioni Il Maglio.

Darczewska, Jolanta (2014): The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study. *Point of View,* 42. Online: www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

Denyer, Sinon – Joo, Kim M. (2019): Kim Personally Supervised 'Guided Weapons' Test, North Korea Says. *The Washington Post,* 04 May 2019. Online: www.washingtonpost.com/world/north-korea-fires-several-short-range-projectiles-south-korean-military-says/2019/05/03/511efe92-6e0f-11e9-be3a-33217240a539_story.html

Department of Defense (2018): *Assessment on U.S. Defense Implications of China's Expanding Global Access.* December 2018. Washington, D.C.: Department of Defense.

Eco, Umberto (2021): Vision '67. In Traini, Stefano: *Le avventure intellettuali di Umberto Eco.* Milano: La Nave di Teseo.

Eilam, Ehud (2016): *Israel's Future Wars. Military and Political Aspects of Israel's Coming Wars.* Washington, D.C.: Westphalia Press.

Eilam, Ehud (2019): *Containment in the Middle East.* Lincoln: University of Nebraska Press.

Eisenstadt, Michael (2017): Information Warfare: Centerpiece of Iran's Way of War. In Hicks, Kathleen H. – Dalton, Melissa G. (eds.): *Deterring Iran after the Nuclear Deal.* Washington, D.C.: Center for Strategic and International Studies. 62–72.

Fabbri, Paolo – Montanari, Federico (2004): Per una semiotica della comunicazione strategica. *E/C, Rivista dell'Associazione Italiana di Studi Semiotici,* 1, 1–27.

Frenza, Maxia M. (2019): *Modelli di comunicazione strategica a supporto dell'Hybrid Warfare: l'apparato di propaganda di Hamas.* Roma: Centro di Ricerca sulla Sicurezza ed il Terrorismo.

Gardner, Hall (2015): *Hybrid Warfare: Iranian and Russian Versions of "Little Green Men" and Contemporary Conflict.* Research Paper 123, Rome: NATO Defense College.

Gaub, Florenze (2015): *Hizbullah's Hybrid Posture: Three Armies in One.* Paris: European Union Institute for Security Studies.

Gordon, Michael R. – Page, Jeremy (2018): China Installed Military Jamming Equipment on Spratly Islands, U.S. Says. *The Wall Street Journal,* 09 April 2018. Online: www.wsj.com/articles/china-installed-military-jamming-equipment-on spratly-islands-u-s-says-1523266320

Gross, Michael L. (2018): *Fighting without Firearms. Contending with Insurgents and Soft, Non-Kinetic Measures in Hybrid Warfare.* MCDC Countering Hybrid Warfare Project. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/717543/MCDC_CHW_Information_Note-Fighting_without_Firearms-March_2018.pdf

Harding, Brian (2019): *China's Digital Silk Road and Southeast Asia.* CSIS, Commentary. Online: www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia

Harel, Amos – Issacharoff, Avi (2008): *34 Days. Israel, Hezbollah and the War in Lebanon.* New York: Palgrave Macmillan.

Harrison, Todd – Johnson, Kaitlyn – Roberts, Thomas G. (2019): *Space Threat Assessment 2019.* Washington D.C.: Centre for Strategic and International Studies.

Herd, Graeme P. – Akerman, Ella (2002): Russian Strategic Realignment and the Post-Post-Cold War Era? *Security Dialogue,* 33(3), 357–372. Online: https://doi.org/10.1177/0967010602033003009

Herskovitz, Jon – Li, Dandan (2019): *China, North Korea Open New Border Crossing Despite Sanctions.* Online: www.bloomberg.com/news/ articles/2019-04-08/china-north-korea-open-new-border-crossing-despite-sanctions

Hicks, Kathleen H. – Hunt Friend, Alice eds. (2019): *By Other Means. Part I: Campaigning in the Gray Zone.* Washington, D.C.: Center for Strategic and International Studies.

Hoffman, Frank G. (2006): *Lessons from Lebanon: Hezbollah and Hybrid Wars.* Pennsylvania: Foreign Policy Research Institute. Online: www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/

Isachenkov, Vladimir (2019): Russian President Putin Hosts Kim Jong Un for Talks on North Korean Nuclear Standoff. *Time,* 25 April 2019. Online: http://time.com/5577801/vladimir-putin-kim-jong-un-meeting-russia/

Kapusta, Philip (2015): *The Gray Zone.* United States Special Operations Command. Online: https://info.publicintelligence.net/USSOCOM-GrayZones.pdf

Katz, Yakoov – Hendel, Yoaz (2011): *Israel vs. Iran. The Shadow War.* Dulles: Potomac Books.

Kaunert, Christian – Wertman, Ori (2020): The Securitisation of Hybrid Warfare through Practices within the Iran–Israel Conflict – Israel's Practices for Securitising Hezbollah's Proxy War. *Security and Defence Quarterly,* 31(4), 99–114. Online: https://doi.org/10.35467/sdq/130866

Marino, Gabriele – Thibault, Mattia eds. (2016): Viralità – Virality. *Lexia. Rivista di semiotica,* 25–26.

McInniss, Matthew J. (2017): Proxies: Iran's Global Arm and Frontline Deterrent. In Hicks, Kathleen H. – Dalton, Melissa G. (eds.): *Deterring Iran after the Nuclear Deal.* Washington, D.C.: Centre for Strategic and International Studies. 25–33.

Min-hyung, Lee (2019): Kim Jong-un Arrives in Vladivostok for Summit with Putin. *The Korea Times,* 24 April 2019. Online: www.koreatimes.co.kr/www/nation/2019/04/356_267718.html

Moss, Daniel (2019): *With Friends Like the U.S., Who Needs Economic Foes?* Online: www.bloomberg.com/opinion/articles/2019-05-23/japan-south-korea-get-reminder-of-how-powerful-china-s-economy-is

NATO 2022 Strategic Concept. Online: www.nato.int/strategic-concept/

Nemeth, William J. (2002): *Future War and Chechnya: A Case for Hybrid Warfare.* Monterey: Naval Postgraduate School.

Office of the Secretary of Defense (2017): Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. Office of the Secretary of Defense, May 2017.

Ottaviani, Marta F. (2022): *Brigate Russe. La guerra occulta del Cremlino tra troll e hacker.* Milano: Ledizioni.

Pak, Jung H. (2018): *Kim Jong-un's Tools of Coercion.* Online: www.brookings.edu/blog/order-from-chaos/2018/06/21/kim-jong-uns-tools-of-coercion/

Quattrociocchi, Walter – Vicini, Antonella (2016): *Misinformation. Guida alla società della disinformazione e della credulità.* Milano: Franco Angeli.

Rusnáková, Soňa (2017): Russian New Art of Hybrid Warfare in Ukraine. Slovak Journal of Political Science, 17(3–4), 343–380. Online: https://doi.org/10.1515/sjps-2017-0014

Sanfelice Di Monteforte, Ferdinando (2020): Scenari di guerra ibrida nel Mediterraneo allargato. *Mediterranean Insecurity,* 22 February 2020. Online: www.mediterraneaninsecurity.it/2020/02/22/scenari-di-guerra-ibrida-nel-mediterraneo-allargato-amm-sq-ferdinando-sanfelice-di-monteforte/

Sanger, Daniel E. – Broad, William J. – Sang-hun, Choe – Sullivan, Eileen (2019): New North Korea Concerns Flare as Trump's Signature Diplomacy Wilts. *The New York Times,* 09 May 2019. Online: www.nytimes.com/2019/05/09/world/asia/north-korea-missile.html

Sang-hun, Choe (2019): Trump Supports Food Aid for North Korea, South Says. *The New York Times,* 07 May 2019. Online: www.nytimes.com/2019/05/07/world/asia/trump-north-korea-food-aid.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer

The Japan Times (2019): U.S., South Korea to Scale Back Large-Scale Spring Military Exercises. *The Japan Times,* 02 March 2019. Online: www.japantimes.co.jp/news/2019/03/02/asia-pacific/u-s-south-korea-scale-back-large-scale-spring-military-exercises/#.XMG1g2hKjcs

The United States Army Special Operations Command (2015): *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014.* Online: www.jhuapl.edu/sites/default/files/2022-12/ARIS_LittleGreenMen.pdf

Thomas, Jason (2020): China's "Fishermen" Mercenaries. *The Weekend Australian,* 02 September 2020.

Walker, Christopher (2018): What is "Sharp Power"? *Journal of Democracy,* 29(3), 9–23.