MADRID SUMMIT 2022 · NATO FACES A CHANGE OF ERA

Nº 8 | 13 July 2022

Emerging Technologies and Balance of Forces

Jose Luis Calvo Albero

Among the many reasons that led to the creation of NATO was the uneven balance of military forces, especially on land, in post-World War II Europe. The Alliance was born as the attempt of some European countries to neutralize this inequality through union and, above all, through the willingness of the United States to demonstrate its commitment to the defense of Western Europe.

Inequality of forces remained throughout much of the Cold War, to the point that NATO doctrine long revolved around the need to use nuclear weapons to compensate for weakness in conventional forces vis-à-vis the Soviet Union and the Warsaw Pact. That situation changed progressively from the 1970s, when there was talk of a Revolution in Military Affairs that could compensate for the number with novel technology and procedures.

The fall of the Soviet Union totally changed the concept of balance of forces, which in the 1990s was simply applied to a balance that was comfortable for both NATO and the heirs of the USSR. This balance was being achieved in a scenario of détente and reduction of forces that lasted until the first years of the twenty-first century.

The progressively more assertive attitude of the Russian Federation and the growth of its military power began to cause concerns in Alliance circles, which developed into a clear sense of threat from the Russian intervention in Ukraine in 2014. The organization's European members were in a particularly worrisome situation, as decades of détente and orientation towards peace and stability operations had eroded many basic military capabilities. The revival of Russian military power and the Kremlin's willingness to use it provoked a reaction, but this was not fast or intense enough to avoid the crisis that led to the Russian invasion of Ukraine in February 2022.

In a Europe shaken by the greatest conflict on its soil since the Second World War, the role of the Atlantic Alliance has been greatly strengthened and the concept of balance and equilibrium of forces has once again acquired the utmost topicality. The performance of the Russian armed forces in Ukraine has been very poor, but that does not erase the certainty that Russia has dared to embark on this adventure precisely because of the perception of political and military weakness in its Western neighbors. The idea of a new security architecture is now emerging, allowing effective deterrence to be exercised without appearing at the same time as threatening.

Technology and the ability to manage it is the key to achieving that goal, although the numbers still matter when it comes to using military force. This chapter will analyze how the Alliance can achieve those capabilities that will lead to a balance of forces that ensures peace in Europe. The war in Ukraine is demonstrating very clearly where the future of European militaries' capabilities, organization and procedures must go and what the key technologies will be in that future.

Technology, information and mentality. Key military capabilities in the twenty-first century

Throughout the twentieth century there are several key moments in which war experiences shaped a novel military model, which broke at least partially with the previous model. One such moment took place in the '70s and '80s, when the American military model was trying to recover from a humiliating defeat in Vietnam. The analysis of a possible war in Europe against the Warsaw Pact led American planners to combine relatively traditional procedures with highly innovative ones. On the one hand, an attempt was made to return to the "war of maneuver" developed by Germany in the last world conflict, which requires speed of decision and a great initiative at all levels of command. On the other, it exploited the capabilities of a technological revolution then in the making, which would later materialize in the modern digital world.

The technology already offered unprecedented possibilities for a level of observation, reconnaissance and target location on the battlefield that had not been known before. In addition, it offered solutions to significantly increase both the range of weapons and their accuracy, through terminal guidance systems. Finally, it also made possible to significantly accelerate the time between locating a target and the moment it is hit by a weapon. Digital networks, then still embryonic, allowed the almost instantaneous dissemination of information between sensors, decision-making bodies and weapons systems.

The model that emerged from this American reaction was called <<Air land battle>> and was adopted by NATO in the 80s as a FOFA (Follow-on Forces Attack) concept. It was enshrined on the battlefield during the Gulf War in 1991 and has since become the symbol of American military supremacy.

In the last years of the Cold War this concept radically changed the balance of forces in Europe. NATO's great strategic problem was always the improbability of stopping the motley armored formations of the Warsaw Pact using exclusively conventional means (Pedlow, 1997:XIV). The resort to tactical nuclear weapons in the face of a massive attack seemed inevitable, but it opened the door to a nuclear escalation of unforeseeable consequences.

The Aeroterrestrial Battle changed that dynamic. The new technologies applied to military systems and the dynamism provided by the initiative of the commanders allowed the enemy deployment to be dislocated in all its depth before it could be introduced into Allied territory. The nuclear option became an emergency response should the adversary decide to make use of it.

During the decades following the Cold War, the Air Ground Battle, successively perfected and modified, was the prevailing model in the Atlantic Alliance for a conventional conflict and was applied to a greater or lesser extent in NATO interventions in Bosnia Herzegovina (1995), Kosovo (1999) and Libya (2011). However, the model was also quite demanding and required technological excellence, highly trained and motivated controls and flexible procedures. The low probability of a conflict in Europe caused the European armies, and even the North American one, to relax and let many basic capabilities deteriorate. The tendency was to focus essentially on guided weapons air operations against adversaries that did not have an advanced air defense system. All the complex inter-arms and inter-army action associated with the Aeroterrestrial Battle was often forgotten, as well as the need to maintain well-trained middle managers in order to effectively use their initiative (Romjue:1984, 55-59).

In addition, both the United States and NATO engaged in conflicts for which the Air-Ground Battle did not work so well. An asymmetrical conflict model very much based on urban guerrillas and terrorism first appeared, and then moved on to the more complex hybrid model, which combined irregular and conventional military actions with the use of non-military tools (Hoffman, 2009). The generalization of the Internet first and smartphones later, multiplied the possibilities of carrying out hostile non-military actions, using either cyberattacks or disinformation campaigns that used digital networks as a vehicle for their rapid dissemination. In this type of attack it is very difficult to identify the perpetrator and, although the damage they achieve is not usually decisive, they do produce a very destabilizing effect. In addition, over-reliance on technology led to dysfunctions, such as the system providing a constant flow of information that was not properly interpreted (Erwin, 2012).

From 2006 onwards, Russia's attitude became increasingly aggressive. The first warning came in 2008 in the war against Georgia and in 2014 the Kremlin showed its willingness to use force to maintain its influence over Ukraine. At the same time, China's economic and military growth was also seen as a threat, not so much in NATO as in the United States. In 2011, President Obama already pointed to China as the most dangerous economic and geopolitical competitor for Washington and launched the idea of strengthening the American economic and military presence and effort in the Pacific (Lieberthal, 2011).

Faced with this new challenge, the reaction of the Atlantic Alliance was uneven, but it acquired a remarkable strength in the United States. The poor results in conflicts such as Iraq or Afghanistan and the revival of the military threat in Europe and the Pacific led to the search for a military solution that, like the Air-Land Battle thirty years earlier, would allow the recovery of US military hegemony.

This reaction was called a third offset strategy or <<Tercer compensation strategy>> (Colom, 2015). The name was derived from what were considered previous strategic concepts to compensate for American military inferiority. The first was the massive nuclear response of the Eisenhower era in the 50s, and the second the modernization and technological drift of the American military arsenal that culminated essentially in the Air-Ground Battle. After the disappointment of the war on terrorism and the loss of conventional capabilities, it was time to react again.

Within this impulse, concepts such as the <<Muldomain Battalion>> appeared, which sought the synchronization of actions in the different domains of the battlefield (air, land, sea, outer space, cyberspace and cognitive environment) or the << Mosaic War>> (Grayson, 2018), which sought the synergy of multiple simultaneous actions of mostly unmanned systems to dismantle the enemy deployment and break the coherence of its action. The truth is that the importance of unmanned systems increased exponentially, especially aerial ones that had diversified to cover functions ranging from reconnaissance to ground attack, passing through electronic warfare or early warning. A novelty in the evolution of these systems was that their development followed two different lines. On the one hand, the traditional one of designing increasingly sophisticated, complex and expensive platforms. On the other, and led by small and medium powers, and even militias and terrorist groups, the trend that sought to employ a large number of simple, cheap and flexible platforms (Marcus, 2022).

This process demonstrated that the practical application of new technologies to weapons systems and military equipment is a complex process. The degree of technological development is as important as the success in designing an appropriate employment doctrine for a new system or being able to integrate "new" and "old" materials into a coherent system (Eaglen & Ferrari, 2020). It has been proven, for example, the good result of integrating fire systems in principle outdated (Cold War artillery) with fire direction systems that combine the action of drones equipped with high-resolution cameras and global positioning systems that immediately transmit the exact location of the piece and the target. The result is a weapon with significantly increased performance at a much more affordable cost than producing a completely new system.

Despite the new developments, the main aspect of the operations remains the interconnection between the different elements of the system formed by the military forces. Reliable and fast communications within a network composed of sensors, decision centers, fire elements, maneuvering units and logistical support are the key to the system. The addition of new technological elements, such as 5G, artificial intelligence or, in the future, quantum computing, may make it possible to overcome the bottlenecks that were generated with the primitive digital systems used during the Aeroterrestrial Battle. Ultimately, the most important thing in an armed force is, as it has always been, its nervous system. The network that allows information to flow quickly, decisions to be timely, and the adversary's ability to react is reduced to a minimum.

Lessons from Ukraine

The Russian invasion of Ukraine in 2022 came as a surprise in many ways. The first of these was that the invasion itself came to pass, thus opening the largest conventional conflict in Europe since 1945. The second was the manner in which it occurred, with an overwhelming weight of conventional forces to the detriment of other hybrid instruments, such as disinformation or cyberattacks, which, although they have manifested themselves during the conflict, have had a rather complementary importance (Fendorf & Miller, 2022). Finally, the poor performance of the Russian armed forces was also surprising, from which much more was expected, especially in terms of their capability to integrate new technologies in the use of fires, unmanned systems or command and control.[1]

The first lesson that can be drawn from the conflict reiterates the importance of networking and the essential nature of command and control systems. Ukraine survived as an independent state because its system of political leadership and military command and control survived the first Russian onslaught. In the eight years that the Ukrainian armed forces had received military assistance from the United States and Britain, the country had not been provided with any heavy weapons system, but its administrative procedures, information management, intelligence

[1] For example, the Russian armed forces were considered leaders in the integrated use of artillery with observation drones and electronic warfare, within the RUK (Complex Fire and Reconnaissance) concept (Grau & Bartles, 2018). However, little of this has been seen on the battlefield.

production, reconnaissance, and command and control (Friedman, 2019). The improvement in management also produced a certain change in mentality that would prove decisive in the confrontation against the Russian army. In the uncertainty and confusion of the first days of the invasion, Ukrainian middle commanders used their initiative to attack the vulnerable points of the Russian deployment, even in small groups of fighters.

They were also very competent in the use of modern technologies with a considerable impact on the battlefield, such as drones (in many cases commercial models adapted to military uses) or cyber defense. In addition, the support received from some private companies in the field of information and connectivity also played a very important role in the Ukrainian success. It is worth noting the internet connection through Starlink satellites or satellite images provided by the Maxar company (Feldscher, 2022).

In contrast, the Russian armed forces showed considerable shortcomings. Its command and control system apparently suffered such serious failures that it forced the use of unprotected communication networks, which resulted in the location and destruction of multiple command posts and the death of several generals (Beaumont & Borger, 2022). The effect on operations was devastating, with obvious difficulties in coordinating the actions of the numerous Russian units in a complex maneuver that unfolded through no less than eleven axes of penetration.

The presumed Russian excellence in the use of its artillery was not revealed until the second phase of the operations in Ukraine, already in mid-April, and only in some sectors of the front where it was possible to achieve a sufficient concentration of these means. Furthermore, unlike on the Ukrainian side, the initiative and leadership capacity of the middle managers was very poor.

On the other hand, it also became evident that the effort in an armed conflict, especially one of medium intensity, far exceeds the purely military sphere and requires a considerable degree of citizen mobilization and the use of all State instruments. In Ukraine, along with the performance of its military forces, the proper functioning of its railway network was essential, both to support military logistics and to attend to the enormous initial flow of refugees. Security forces and intelligence services also played a prominent role in neutralizing groups of saboteurs in the early days of the conflict. Civil defense managed to reduce the consequences of the damage caused by Russian bombing and the government activated an authentic army of "hackers" focused on both the cyber defense of State networks and the attack against Russian interests in the network (Shore, 2022). Likewise, many volunteers played a prominent role, both in supporting the evacuation of vulnerable people and in the management of refugees or even on the battlefield, as the improvised unit of drone experts that helped slow the Russian advance on Kiev. (Shoaib, 2022). Security and defense are activities in which the State must act comprehensively, managing and coordinating all available resources, and even generating new ones. To this end, as stated above, the existence of a secure, reliable and flexible command, control and communications system is essential.

In short, the lessons learned from the war in Ukraine are oriented, on the one hand, towards the need to reinforce the central elements of any defense system, especially the nervous system made up of the command and control, communications and intelligence systems, integrated into digital networks and managed with a proactive and open mindset. On the other hand, it also points to the need to consolidate comprehensive security systems that make it possible to combine purely military capabilities with the rest of the State's instruments with security applications, from the police forces to the civil protection system, including communications networks, cybersecurity and the healthcare system. Integration and interconnection, driven by the possibilities of new technologies, are the key concepts in terms of security and defense capabilities in the 21st century.

What will NATO need in 2050?

Achieving credible deterrence and a sustainable and efficient balance of forces always requires some combination of four essential factors: numbers, organization, technology and motivation. It is very difficult to always have an adequate proportion of each of these factors, so it is usually necessary to compensate for deficiencies in some with excellence in others. Among NATO members, it is clear that good organization and cutting-edge technology are more likely to be available than large forces or exceptional motivation.

The consequence is that what offers the greatest chance of success must be strengthened, but without forgetting what is weakest, since there are thresholds that, once crossed downwards, can cause the collapse of the entire system. For example, clearly insufficient motivation can completely nullify the effects of technological excellence, leading a society to give up before its superiority in technology has a chance to manifest itself on the battlefield.

In any case, the Alliance's effort to improve its organization and develop its technological level should be aimed at reinforcing the two key factors mentioned above: interconnection and integration.

Regarding interconnection, there are two technological niches that are likely to become decisive during the 21st century. The first of these is the development of artificial intelligence which, combined with 5G and 6G, will allow increasingly greater autonomy for robotic military vehicles and systems, will improve the speed and precision of decision-making processes in operations and will revolutionize activities such as cyber defense, giving a pace to actions in this domain that would be impossible for human operators. The second technological niche focuses on quantum computing which, as a first consequence, will dramatically modify the security of military communications, offering whoever masters this technology first the possibility of enjoying impenetrable encrypted codes and, at the same time, the ability to break enemy codes. As a second consequence, quantum computing will contribute decisively to the development of a more capable artificial intelligence with a greater degree of autonomy.

Interconnection should facilitate the development of a model that extends the possibilities of the traditional Air-Land Battle to a scenario in which action must be taken simultaneously in multiple domains and using an increasing number of unmanned platforms. Again, we must remember that it is not just about the technology but about the mentality when using it. Technological excellence is of little use without the appropriate component of decision-making capacity, imagination and initiative in system operators.

It must also be remembered that the consequences of a technological revolution are not fully apparent until the advance in technology is translated into simple, sustainable and easy-to-use products. Although complex and expensive combat platforms will still be necessary in some cases, the future probably lies in simpler, more accessible and cheaper products. Swarms of small drones, for example, may have a more promising future than complex manned systems.

In terms of integration, NATO must be able to make the leap from mere defense to security. This is a complicated step because it would imply that the organization equips itself with civilian capacities that it does not currently have or does not have the capacity to manage, even though its member states do have them. The most realistic solution is probably not to make NATO a more complex organization than it already is, but rather to improve its ability to interact with actors that do have this type of civilian capability, be it allies and partners, or supranational organizations such as the European Union. In fact, cooperation between NATO and the European Union, which possesses diplomatic, legislative (signing of treaties, enactment of laws) and financial capacities that the Alliance lacks, is presented as one of the most promising possibilities for future European security . The need for integration in security and defense is not limited only to the internal structures of each State, but also extends to multinational collaboration or between international organizations.

Although technological excellence and organizational reform to maximize its potential are the most promising areas of development for the Alliance, it is important to maintain at least an acceptable level in other, weaker factors. Perhaps the most sensitive is motivation. Alliance members are developed countries with more than acceptable standards of living and societies not inclined to face the sacrifices of armed conflict. This has an important influence on the effectiveness of deterrence. It is of little use to have powerful military forces if the society that sustains them does not have a minimum degree of resilience.

In NATO countries, this social resilience varies, but it is by no means exceptional. One of the fundamental tasks of the Alliance is to strengthen it or, at least, prevent it from deteriorating further. One way to achieve this is to improve the ability to deal with strategies precisely designed to break the resilience of society. Among them, cyberattacks, disinformation campaigns or terrorist attacks, which target civil society, should be highlighted.

Another aspect that must be taken into consideration is the number, referring to the amount of military capabilities available. Technology and good organization can make up for limited forces, but only up to a point. There are critical levels below which operational capacity crumbles. The importance of reserves, mobilization and the availability of sufficient supplies and ammunition stocks has been demonstrated in the Ukraine war. The modern battlefield is highly lethal and consumes extraordinary amounts of ammunition, fuel and equipment so quantity still matters, especially in a conflict that lasts more than a few days. Although it may seem like a throwback to 19th century military strategy, mobilization capability still counts heavily in exerting credible deterrence and achieving a balanced balance of forces.

Conclusions

It is very likely that the end of the war in Ukraine will see a renewed effort to build a new security architecture in Europe. That effort will include a "soft" part focused on de-escalation, disarmament, and confidence building measures and a "hard" part focused on deterrence. The bad experience of the Ukrainian conflict, resulting in part from a failure of deterrence, will lead to more attention being paid to this aspect of security.

The deterrence must be credible but not threatening. Sufficient to avoid temptations to use military force, but also contained and limited, to avoid the impression that an aggression is being prepared. A balanced and reasonable balance of forces is one of the essential conditions for maintaining peace in any part of the world that is home to several powers with diverse interests.

Since the 1970s, the Alliance's deterrence capacity has been based on technological superiority, a more efficient military organization and more modern procedures. In the 21st century, it seems logical to continue along this line, although the experience of recent conflicts reminds us of the need not to forget other aspects of security, such as the resilience of society or a sufficient volume of forces and supplies to feed them.

To maintain technological excellence, NATO must essentially work on improving the interconnection of its forces, which has traditionally been a decisive factor in military operations and is even more so in the digital age. The adequate application of new technologies such as artificial intelligence, 5G and 6G or quantum computing will allow data transmission times to be reduced, faster decisions, beat targets with greater opportunity and precision, reduce the vulnerability of own networks and, finally, achieve an effect of disintegration of the adversary's coherence, as a result of the action of multiple network systems, many of them unmanned.

In terms of organization, the Alliance's greatest challenge is to move towards a more comprehensive security system, extending the purely military aspects that have been the cornerstone of the organization until now. It is difficult for NATO to evolve into a more complex organization, with the capacity and competence to manage other security instruments more typical of States, but it can adapt its structures and procedures for better interaction. Collaboration with the European Union, an actor with multiple security instruments that NATO does not possess, appears as one of the most promising possibilities both for the Alliance itself and for the future European security architecture.

Finally, we must not forget that the effectiveness of any security and defense structure rests on the competence and motivation of the people who manage it. Technological and organizational excellence, as well as the integration of multiple security elements, requires not only innovative equipment, procedures and techniques, but also a new mentality, capable of extracting the maximum performance from new systems. NATO was created to protect a culture that prioritizes personal freedom, initiative and creativity as essential qualities of a society. Those were its best weapons in the harsh period of the Cold War and will continue to be so in the uncertain 21st century.

References

Beaumont, Peter & Borger, Julian, (2022) "US intelligence helping Ukraine kill Russian generals, report says", *The Guardian*, 5 mayo de 2022, https://www.theguardian.com/world/2022/may/05/us-intelligence-helping-ukraine-kill-russian-generals-report

Colom. Guillem (2015), "Rumsfeld revisited: La tercera estrategia de compensación estadounidense", *Revista UNISCI / UNISCI Journal* , Nº 38 (Mayo / May 2015), https://www.ucm.es/data/cont/media/www/pag-72452/UNISCIDP38-3COLOM.pdf

Eaglen, Mackenzie & Ferrari, John, (2020), "Use Legacy Systems as Tech Playgrounds for Innovation", *Breaking Defense*, November 19, 2020, https://breakingdefense.com/2020/11/use-legacy-systems-as-tech-playgrounds-for-innovation/

Erwin, Sandra I., "Too Much Information, Not Enough Intelligence", *National Defense*, 05-01-2012, https://www.nationaldefensemagazine.org/articles/2012/5/1/2012may-too-much-information-not-enough-intelligence .

Feldscher, Jacqueline (2022) "The Ukraine War Is Giving Commercial Space an 'Internet Moment'", *Defense One*, 7 abril de 2022, https://www.defenseone.com/technology/2022/04/ukraine-war-giving-commercial-space-internet-moment/364101/

Fendorf, Kyle & Miller, Jessie, (2022), "Tracking Cyber Operations and Actors in the Russia-Ukraine War", *Council on Foreign Relations*, March, 24, 2022, https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war

Friedman, Uri, (2019), America Hasn't Always Supported Ukraine Like This, *The Atlantic*, November 21, 2019, https://www.theatlantic.com/politics/archive/2019/11/how-vital-us-military-aid-ukraine/602407/

Grau, Lester W. & Brtles Charles K. (2018), "The Russian Reconnaisance Fire Complex comes of age", *Oxford Changing Character of War Centre*, May 30, 2022, http://www.ccw.ox.ac.uk/blog/2018/5/30/the-russian-reconnaissance-fire-complex-comes-of-age

Hoffman, Frank G.(2009), "Hybrid Warfare and Challenges*", JFQ* / issue 52, 1st quarter 2009, https://smallwarsjournal.com/documents/jfqhoffman.pdf

Grayson, Timothy, (2018), "Mosaic Warfare and Multi-Domain Battle", Youtube video, DarpaTV, https://www.youtube.com/watch?v=33VAnIEjDgk

Lieberthal, Kenneth, G. (2011), "The American Pivot to Asia", *Brookings Institution*, December 21, 2011, https://www.brookings.edu/articles/the-american-pivot-to-asia/

Marcus, Jonathan (2022), “Combat drones: We are in a new era of warfare - here's why”, *BBCNews*, 4 February 2022, https://www.bbc.com/news/world-60047328

Pedlow, Gregory W. (1997) “NATO Strategy Documents 1949-1969” Supreme Headquarters Allied Powers Europe, 1997, https://www.nato.int/docu/stratdoc/eng/intro.pdf

Romjue, John L. (1984), *From Active Defense to Air Land Battle: The Development of Army Doctrine 1973 – 1982*, United States Army Training & Doctrine Command, Fort Monroe, Virginia.

Shoaib, Alia (2022) “Inside the elite Ukrainian drone unit founded by volunteer IT experts: 'We are all soldiers now.”, *Insider*, 9 abril de 2022, https://www.businessinsider.com/inside-the-elite-ukrainian-drone-unit-volunteer-it-experts-2022-4?r=US&IR=T

Shore, Jennifer (2022), “Don’t Underestimate Ukraine’s Volunteer Hackers*”, Foreign Policy*, April 11, 2022, https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army