WAR IN THE FUTURE — NEW AND OLD CHALLENGES

LARS BANGERT STRUWE, SECRETARY GENERAL, PHD,
DANISH ATLANTIC COUNCIL

ATLANTSAMMENSLUTNINGEN

WAR IN THE FUTURE — NEW AND OLD CHALLENGES

Lars Bangert Struwe, Secretary-General, PhD,
Danish Atlantic Council

-

1. edition 2022

ISBN 978-87-87008-98-3

-

Frontpage Illustration by
L. Vallet & Henriotin in Henry de Graffigny
"Aventures extraordinaires d'un savant russe".
Layout by booksandmore.one

-

1. INTRODUCTION

"To be prepared for war is one of the most effectual means of preserving peace."

GEORGE WASHINGTON, 1790

In these months, rearmament, especially of the European parts of NATO, is starting. The question for politicians and the military becomes, what should we invest in? What type of war are we facing? This report will seek to describe some of the changes facing war.

In the last twenty years, new types of war, hybrid war, and cyberwar have been discussed. However, the Ukraine war shows very clearly how new and old technology are mixed and how different types of warfighting happen simultaneously. We see war in cyberspace as well as tanks, infantry, and planes deployed on the battlefield. NATO must be able to do this in the future.

The North Atlantic Treaty Organisation (NATO) currently faces changes in warfare equivalent to the changes that occurred between 1914 and 1918. The armies with which the European armed forces went to war in August 1914 could very well have been recognised by General Napoleon or his adversaries in 1814. In 1918, the armed forces underwent dramatic change. The skies emerged as a new warfighting domain and the war at sea also saw changes, including the first original use of submarines. Simultaneously, machine guns against mass armies changed the rules on the battlefield. These factors caused changes on all levels of strategy, from the sub-tactical level to grand strategy. The same kind of changes are underway for NATO's armed forces as well as the member states' civilian leadership.

Looking forward to 2040 is a difficult task, though we can now already predict some of the changes — they are underway, they are based on research performed during the last 10 to 20 years, the technologies exist and the domains are known. However, the unknown factor is how the individual elements will work together. Further, there remains the risk that brand new and unforeseen technologies may arise.

NATO is based on two pillars: firstly, a command structure and, secondly, and probably most importantly, an idealistic thought that had to become a reality. NATO is more than merely the words of Article Five. As the alliance's name states, the North Atlantic Treaty Organisation is built on a treaty, an agreement between equal partners. The preamble establishes that NATO is a mindset with a framework based on peace, freedom, democracy, rule-of-law, and individual liberty.

These two pillars will carry NATO into the future; however, its investments in warfighting capability must be based on its overall approach to the future, including the individual member states' investments in modern and contemporary capabilities.

The purpose of war will not have changed in 2040: *'War is thus an act of force to compel our enemy to do our will.'*[1] However, the means available to force our enemy's resolve will have changed. One of the best examples to help us understand this change in the means is the military revolution of the First World War. This war fundamentally changed

World War I changed war in the same way we can see it in the future. New military domains emerged, and at the battlefield, soldiers witnessed these changes. Photo Frank Hurley/National Library of Australia.

warfare and international politics. For politicians and military leaders, many of the inventions and accompanying changes had already taken place before the war, though the changes were implemented or accelerated during the war.

NATO sees four characteristics of technologies that will define combat-critical military technologies in the future: Intelligent, interconnected, distributed, and digital.[2] In its work towards 2030 with Emerging Disruptive Technologies (EDT), NATO is focusing on seven technologies. For each of these technologies, separate strategies are developed. The technologies are as follows: artificial intelligence (AI), data and computing, autonomy, quantum-enabled technologies, biotechnology and human enhancements, hypersonic technologies, and space.[3]

Based on the above approach, this report will examine the future of NATO warfighting and is based on the following assumptions:

- For the next 20 years, we will live in some kind of international crisis where the focus will constantly shift from one crisis to another. Such a permanent international crisis is the symptom of the superpower rivalry we will see in the next 20 years.
- To distinguish war from peace is no longer a clear possibility. We are living in a grey zone where distinctions vanish. This has been described as hybrid warfare or special warfare.[4]
- Geography has returned — and at the same time, geography has disappeared. This means that future threats can arise from powers physically close to NATO-states, such as Russia, and that the cyber domain represents a threat without a geographical dimension. A particular challenge will be

in for form of threats from states outside of the ordinary NATO Area of Operations, such as China, as the NATO Secretary-General pointed out in August 2019.[5] Threats to a NATO state can now originate from almost anywhere in the world.

- Technology becomes more and more expensive, while at the same time, technology is cheap and can be developed anywhere.
- Space has emerged as a warfighting domain in its own right and as a key enabler for almost all terrestrial operations.

1.1 MILITARY TRANSFORMATION

One of the most remarkable characteristics of NATO is its ability to reinvent itself continuously. In his speech to the US Congress in April 2019, Secretary Jens Stoltenberg stated, 'NATO is the most successful alliance in history because we have always been able to change as the world changes.'[6]

The sources of military transformation can be multiple and include '*cultural norms, politics and strategy, and new technology.*'[7] NATO reinvented itself — or its strategy — several times during and after the Cold War. Had NATO not reinvented itself, it would have ceased to exist. Reinvention can be caused by critical junctions, where a shock animates a new development.[8] This has been the case for NATO, where transformation was caused by either political and strategic shifts or by the advent of new technology. During a shock or in a time of crisis, NATO has shown itself able to meet

Humans and autonomous machines operating on the battlefield. DARPA.

and overcome challenges. In the future, it is more uncertain whether the time necessary to secure a quick adaption to such challenges will be available.

One means of sheltering NATO against inevitable future shocks and, hereby, securing NATO's instrument of power fast enough is a combination of increasing existing capacities and the development of new technologies. To safeguard themselves, NATO states must expand their militaries. The budget cuts since the end of the Cold War, and especially after the financial crisis of 2008, in both the NATO Command Structure and NATO states' armed forces, have resulted in armed forces with a limited capacity, to the extent that it challenges NATO's deterrence strategy.

The NATO states' technological advantage is undermined by the states having such few capabilities that a possible enemy, by means of abundant mass, can circumvent technological inferiority. An example of this is China's commitment to mass in missiles, which can make it difficult for the United States to maintain its dominant position, particularly in Asia.[9]

In the past, Western military transformation was focused on and provided an opportunity to:

1. change tactics based on newly available technology,
2. change the size of the armies/navies,
3. establish new strategies,
4. impact on society by establishing a new administration that was able to handle a new military,
5. an escalation of the area of operation.

These were the main elements in the so-called Military Revolution in the 16th and 17th centuries.[10] Western domination of the world from around 1500 to 2000 was largely based on this military revolution. The five elements can be recognised in the changes to warfare that occurred during and right after the First World War. They can also be recognised in the transformation of NATO since 1990. In NATO, the transformation has been driven by a change in politics and strategy, the United States, and constrained or few resources among the other member nations. The changes themselves have been based on the experiences of American forces and how they are structured.[11]

The necessary military transformation/revolution of NATO towards a capable warfighting machine in 2040 should be based on a well-thought-out strategy that relates to the five elements outlined above. The five elements can also be used as a checklist.

This report will describe these elements of the future changes in security policy, strategy, and new technology to provide a platform for military procurement in each NATO state.

The Battle of Breitenfeld in 1631 was part of the military revolution, in which, among other things, the armies grew, new technology was introduced and larger armies operated in larger areas.

2. CHANGES IN THE GLOBAL SECURITY SYSTEM

Currently, the world is changing from the 'New World' — the world we saw from around 1500, built on the Western military revolution, The Age of Discovery, etc — to a multipolar and, perhaps most importantly, multi-civilisational order encompassing the whole globe.[12] The challenge in many ways will be to channel and control *'divergent historical experiences and values … into a common order.'*[13]

Present population growth in Asia is a pressing matter. By 2027, India is projected to overtake China as the world's most populous nation. However, by 2050, Africa will have the world' s largest population. This means that over the next 30 years, we will see a shift — as we are currently witnessing in Asia — which will be followed by a shift to Africa as far as population size is concerned. This will probably impact the emergence of strong powers in Africa. Whether this means that, for example, Nigeria or South Africa may develop into great powers nevertheless remains uncertain. However, it seems quite likely that these changes in population growth will significantly impact security policy in the form of both migration and the risk of conflicts related to food and water.

From today, and for the next 20 to 30 years, the world will see a great power competition, one which we have not seen for many years. The USA and China will be the main actors, though Russia and increasingly India will take part in the competition for influence on the world political stage. It will be a competition on all levels, from soft power and economics

to hard military rivalry. It will also be a competition of values. On the one side lies the Western values of democracy, human rights, and the right to free speech; on the other side lies a rising China that insists on social and economic rights — but not political rights.[14] We can expect NATO's values to be challenged to an unprecedented degree.

2.1 GREAT POWER GAME — PENTARCHY

The new great power game is played by the USA, China, Russia, an emerging India, and perhaps the EU. This could form a kind of pentarchy, as seen in the 18th century.[15] This was a rather unstable state of affairs where the European powers changed alliances between both smaller countries and between the great powers. The outbreak of the Prussian Seven Years' War in 1756, for example, can to some extent be traced to shifts in alliances—a switching of partners known as the Diplomatic Revolution — where Austria shifted its allegiance from the United Kingdom to France, while Prussia and the United Kingdom became allies. Over the next 20 years, we can again expect to see this type of shift in alliances.

PENTARCHY

The modern pentarchy consists of the United States, China, Russia, India and the European Union. Five powers that ally themselves with each other and are in conflict with each other.

The two most powerful states will be the USA and China, and the other states will seek to benefit the most from this. Despite an increase in ties between Russia and China, Russia remains a minor partner for China. Therefore, it is possible in the not-too-distant future that Russia will seek to ally itself with the USA or the EU to maximise its benefit. This, of course, will require a solution to the current Ukraine war, and that Russia sees itself more threatened by China than by the West. Right now, it is a utopia, but history has shown us that rapid alliance changes and policy changes are possible and have actually happened. It happened, for example, with US-China politics in the 1970s.

It is a classic alliance game that we will face, where one seeks to optimise one's position by switching alliance when one's ally gains more from the alliance than oneself — or when it is possible to secure a better deal from others. This means that the USA and China will establish themselves as opposite poles, while Russia, India, and the EU will be able to operate between them. However, the vast majority of EU member states are also members of NATO. We share common values with the United States, which provides a very strong connection across the Atlantic Ocean.

One challenge for the actors in the new great power game will be the risk of being overstretched. Throughout history, it has been a common dilemma for the leading great power that it was obliged to invest more and more in its military if it wanted to safeguard its position. That led to a downward spiral for the greatest power in any given period.[16]

2.2 NEW ACTORS IN THE GAME

In addition to the usual state actors, new (or actually old and well known) actors are emerging: from terrorist groups to non-governmental organisations (NGOs) to private industry. They all seek to influence politics, be it peacefully or through the use of force. NGOs and terrorists are well known to the public as actors in international politics. The same can be said about technology companies like Google, Ali Baba, Apple, and the like.

What is less known is how international companies have used or considered using military power in the last few decades. Up until the 19th century, companies like the English East India Company or the Dutch East India Company had very large military units at their disposal — of which they made ample use. A modern example is how Jardine Lloyd Thompson Group (JLT), which insures 14 per cent of the world's commercial shipping fleet, in 2010 proposed the establishment of a private navy comprising 20 patrol boats. Their purpose would be to escort ships passing through the Suez Canal and the Indian Ocean and respond to pirate attacks in the area.[17] In Sierra Leone, mining companies hired private military companies (PMC) to fight rebels, and the military's deployment of the PMCs was an important element of peace-making in Sierra Leone.

The Wagner Group is a modern version of mercenaries. Here, we see a group of more or less organised soldiers working with some affiliation with the Russian state.[18] The deployment of the Wagner Group in Syria is an example of how mercenaries are being used as deputies for the states in the new great power conflict. For the next many years, we will be deploying this type of group in proxy wars worldwide.

The war in Ukraine could be an example of future war. Here we have seen that private individuals have taken up the fight against Russia—either in the form of joining the Ukrainian Foreign Legion or in more or less organised networks that, for example, can carry out cyberattacks. This mixture of the state monopoly on violence and then the private sector may well become part of the future battlefield. Private companies can support the state with, for example, cybersecurity, where we have seen Romanian companies that have teamed up with the Romanian National Cyber Security Directorate (DNSC).[19] This is an expression of the fact that the companies are being bought to provide a security service and that there is a common denominator between civilian and military critical infrastructure. Therefore, during a crisis or a war, the private business sector can be affected directly or in the form of a spill-over from, for example, cyberattack.

In other words, it is very likely that operators in upcoming theatres of war will not be limited to be states but will also include other actors who, in some cases, will exercise states' monopoly of power and sovereignty. The challenge for these actors will be to physically build bases if classic military power is discussed. Therefore, these actors will be interested in using, for example, the cyber domain, where normally much-needed physical military facilities such as ports, barracks, or airfields are not required. This makes the actors less vulnerable and provides them with a flexible and simple way of operating. In weak states, however, these actors will be able to undertake constructions that are far more reminiscent of classic military organisations.

2.3 THE BATTLEFIELD IN THE NEW SECURITY ORDER

Over the years, it has been debated where NATO forces should be deployed and operate. Is the Transatlantic Area of Responsibility the limit of NATO operations, or may NATO work beyond the border of the Transatlantic Area of Responsibility? It was debated whether NATO should engage in the French operations in

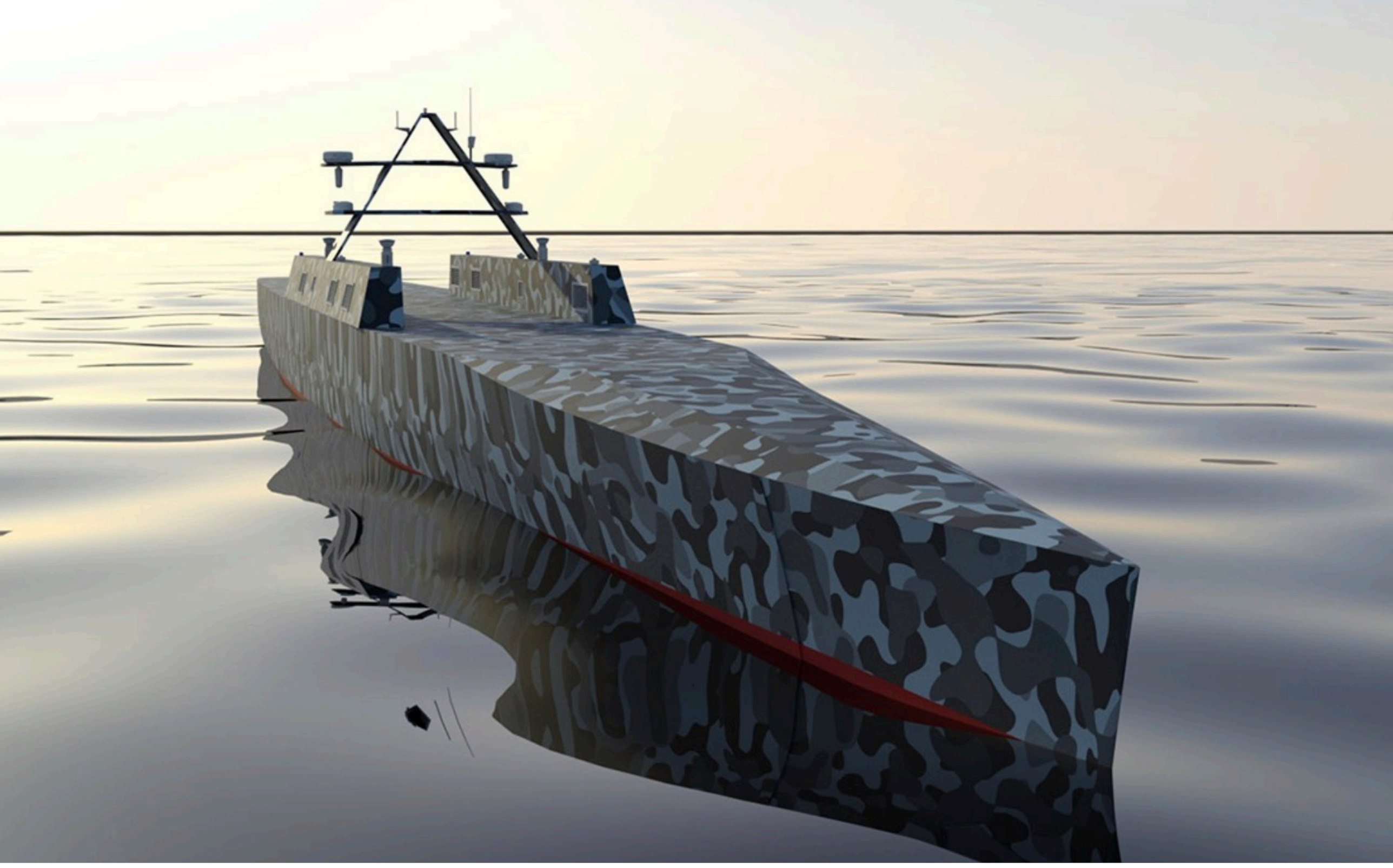
Destroyed Russian tanks in the Sumy region, Ukraine, March 7 2022. Photo Irina Rybakova/Press service of the Ukrainian Ground Forces

Algiers in the 1950s, in the US-led operations in Vietnam in the 1960s and 1970s, and lately in the US-led operations in Afghanistan. We all know the historical facts. Therefore, we all know that NATO adapts accordingly, respecting the past and accepting the present in order to meet the future — and that is the key to NATO's survival as a defence alliance.

The battlefield of the future will consist of all five military domains at the same time. Sea, land, and air will remain very similar to themselves, while the deployed forces will be complemented by the latest technology, that is, primarily robots guided by AI. Moreover, the development will be fast-passed — speed will be everything.[20] There are (at least) five different issues that will change the future battlefield:

- cyber technologies,
- space,
- cities,
- climate changes, including their direct or indirect influence on the Arctic Region,
- attacks on allied countries outside the Transatlantic Area of Responsibility.

All NATO countries must see themselves as being under a continued cyberattack. The list of attacks since 2006 is alarming,[21] and no one should consider themselves exempt from cyberattacks. Until recently, many analysts tried to distinguish actions taken in cyberspace from those taken in the 'real world'. Israel changed that in 2019. Israeli Defence Forces tweeted that a real-time missile attack countered a hacker attack.[22] This means that the various military domains can no longer be separated and that cyberattacks will take place continuously, including in times of peace.



Concept Design of the DARPA No Manning Required Ship (NOMARS) X-Ship program. Photo Serco.

On the other hand, NATO itself can make use of cyber capabilities both defensively and offensively. In 2016, the US was considering using a cyber response to the Russian hacking of Hillary Clinton's emails. Being discussed, among other things, was a closure of the Russian financial system. The proposal was rejected but illustrates the possibilities which cyber operations offer.[23]

Space has for a long time been a military domain. Until recently, peace has reigned in space, and space has only been used to obtain intelligence, gather information, and as the basis of satellite-based navigation systems. This state of affairs, however, is changing dramatically. The USA, China, Russia, India, and France have launched new space research programmes.

The new benchmark for superpowers is whether they can deliver kinetics or use directed-energy weapons in space,[24] In other words, whether they have the wherewithal to shoot down satellites or shut them down by other means. From a long-term perspective, another benchmark will be the ability to use satellite-based systems to paralyse or attack operations on the ground. This is not the Ronald Reagan-era Star Wars programme that was meant to *'give us the means of rendering these nuclear weapons impotent and obsolete.'*[25] Rather, the new Star Wars programme is a means of shutting down communications and navigations systems and, in such a manner, blindfolding your opponent.

Warfare will also take place in space. China currently conducts research on orbit capacities, where the focus now is on the maintenance of satellites in space, but in time these capacities can be developed into orbital threats.[26]

Thus, when we combine the development of cyberspace with the development of space programmes, there is a risk that the increased digitalisation and dependence on cyber technologies and space will present a very clear vulnerability in this area. It has the very unpleasant consequence that NATO forces must learn to operate without satellite-based military systems such as GPS, various communications systems, or satellite-based intelligence. Therefore, NATO must protect both these systems/domains and train, practise, and learn to operate on the battlefield without them. As far back as World War One, Great Britain discovered that control over the cables to North America was vital.[27]

Since the establishment of cities, there has been a movement from rural areas to cities. It is very clear that cities have always been the centre of social, economic, and political activity. Today, a continued concentration of people in urban areas is taking place, and an increasing portion of the world's population lives in cities.[28] This drives domestic and international migration. The number of megacities with a population of more than 10 million is steadily growing. The last 100 years of warfare show how complex urban fighting is.

Cities, on the one hand, are a military target — as has been seen for centuries. The capital or other cities form strategic hubs. On the other hand, cities are an obstacle where fighting can take a long time and delay operations. The Americans experienced this in Iraq, and at the time of writing, the Russians were experiencing it in Ukraine. The growing cities — and the growing number of cities — present a serious problem for the armed forces. Both urban warfare and sieges are back in the discussion of strategy.[29] In the last 30 years, war has been taken into cities like Bagdad, Basra, and Grosnyj. Cities are vulnerable to threats from terrorists, gangs, or militias, and the operating environment is difficult.[30] This means that sieges have once again become part of military strategy, where one wants to conquer the city but not conduct a battle from house to house.

There will always be a very high risk that civilians will be harmed during military operations in cities. Furthermore, maintaining situational awareness as well as locating the adversary in cities is extremely difficult. There is no quick fix, though a large amount of research, especially from the USA and the Israel Defence Forces (IDF), on how new technologies can help soldiers fight in cities is being undertaken. At the same time, a completely different problem is that megacities can potentially develop into independent entities able to challenge states. Cities and megacities are perhaps the most challenging battlefield for NATO in the coming years.

Climate change will be a driver of human insecurity.[31] Research has shown that *'worldwide and synchronistic war–peace, population, and price cycles in recent centuries have been driven mainly by long-term climate change'*.[32] Climate change can lead to conflicts; however, it remains uncertain whether climate change will function as a direct trigger of conflict.[33]

Climate change will surely alter the operational environment. During the Little Ice Age, climate change made it possible for Swedish troops to cross the ice-covered sea on foot and attack the Danish capital, Copenhagen, in 1658. In Chinese history, there seems to be a direct connection between changes in climate and war.[34] Climate change will also challenge NATO forces outside the ordinary conflict spectrum. During and immediately after natural disasters, the military is often the only entity with the capacity to take rapid action.[35] This means that climate change can lead to greater use of NATO's military resources, deployed in disaster areas to both help or assist and avoid the catastrophes, resulting in negative security policy developments.

For NATO, the clearest immediate impact of climate change is the melting of the ice in the Arctic Region. Consequently, the North Atlantic and the Arctic Region will become navigable to a greater extent than previously possible. However, the Arctic Region will continue to be a very difficult area in which to operate. Operations in the area will typically occur in the sea or air domains. Nevertheless, as we saw during the Cold War, it will be crucial to have control over the region. This holds especially true with regard to the sea lines of communication (SLOC), in terms of bringing reinforcements to Europe, the containment of Russia and maintaining radar facilities in Greenland — the latter being part of the US missile warning system. There is a risk that the Arctic Region will be affected by spill-over from conflicts elsewhere, involving China or Russia. As a battlefield, it is perhaps one of the most terrifying thoughts. The lessons from the Second World War show how difficult it is to operate in the area: only very few can survive warfighting in this extreme environment.

In addition to the aforementioned changes in the battlefield, new regions may be the subject of NATO operations. It can by no means be ruled out that virtually the whole world could become NATO's area of operation. The most likely opponents to the United States in the next 20 years will be Russia and China. Depending on how and where a conflict with China erupts, there is a risk that NATO will have to operate in, for example, the South China Sea.

Communication via cable has since at least World War I been subject to eavesdropping. The Eastern Telegraph Company's undersea network. Photo Atlantic-cable.

3. WAR OR PEACE

War between states — especially so-called great power war — is not within the personal experience of decision-makers, officers, or researchers today. They will, therefore, find it easier to dismiss as a real risk.[36] In the period from 1946 to 2014, the number of interstate wars has diminished.[37] One might be led to believe that interstate wars will disappear in the 21st century, should this trend continue linearly. Yet this will be a dangerous assumption, as it does not reflect the growing superpower rivalry between the United States, China, Russia, and possibly India by 2040. The Ukrainian Crisis in 2022 shows that we cannot completely dismiss the risk of a great power war.

To understand the present, one must know the past and prepare for the future. Looking into the future is possible only when the past is known and when it is known how to use the past. As an alliance, NATO is based on the lessons which the allied nations learned from two world wars. These lessons were used to form the new alliance politically and militarily. NATO is based on warfighting lessons.

3.1 DETERRENCE

The most important lesson was the need for a unified command structure that could lead combined and joint operations in multiple theatres of war. The allied victory in Europe in 1918 and 1944-1945 was based on these principles.[38] The Supreme Allied Commander Europe (SACEUR) is the living proof of this. At the same time, political leaders learned that an alliance should be formed in a time of peace to deter from war — and to be prepared for war.

The most important lesson from the Cold War was that deterrence works, but it must not be oversold.[39] In 1946, Bernard Brodie wrote, *'Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them.'*[40] This was his view of nuclear deterrence. Today, we know that deterrence only works to some extent.[41] Deterrence was — and is — based on the assumption that the whole NATO system works. During the Cold War, NATO defence planning, contingency planning, exercises, operational training, readiness, resilience, military force structure, command structure, and MAD (the mutually assured destruction strategy) all worked and established a reliable deterrence. NATO's deterrence was based on a mix of conventional and nuclear deterrence.

Russia has created a new form of nuclear deterrence. This was based on two deeply concerned findings:

1. Russia saw its weaknesses in military operations in the 1990s.

2. At the same time Russia saw the force and new technologies of the West.

Based on these findings the Russian military doctrine of 2000 states that nuclear weapons can be used in response to a conventional attack on the Russian Federation.[42] In the Western world, we have seen a larger — and sometimes somewhat uncertain — discussion about whether Russia has introduced an 'escalate to de-escalate' doctrine.[43] This means that it is believed in the West that Russia, in the event of losing a conflict, is ready to escalate it with a nuclear weapon in order to be able to stop war and de-escalate the situation. In itself, this insecurity about Russian doctrines in the field constitutes a deterrent.

President Vladimir Putin has understood how to employ the nuclear deterrent during the war in Ukraine, where he has put nuclear forces on increased alert.[44] This new way of playing on nuclear deterrence requires a new doctrinal approach from NATO. It is unheard of to use the nuclear deterrent against states that do not themselves have nuclear weapons, and it can create a whole new dynamic where states that see themselves threatened to a much greater extent will seek to seize chemical, biological, radiological, and nuclear (CBRN) weapons as a deterrent.

In the future, deterrence must be created in all five domains. It will be more than difficult, and potential opponents will bet that they are able to tip the balance by affecting at least one of the domains, possibly before a war breaks out. First strikes — surprise attacks such as the Blitz, the Japanese attack on Pearl Harbour, or Egypt and Syria's attack on Israel in 1973 — are scenarios that NATO must study closely, especially after Russia has shown its capability to shoot down satellites.[45] These studies should involve how an opponent of NATO can, with active use of both the cyber and space domains, blind or paralyse NATO for a short or lengthier period of time, and how NATO can continue to fight in such a situation or environment.

3.2 THE GREY ZONE BETWEEN WAR AND PEACE

The distinguished strategist Antoine-Henri, Baron de Jomini, wrote in 1838 that *'We will suppose an army taking the field: the first care of its commander should be to agree with the head of the state upon the character of the war.'*[46] It sounds very reasonable, though too often, the question of what kind of war are we facing has not been raised. Too often, the

military and political leadership have not been able to agree on this fundamental question. In connection to this, they have been unable to ascertain the ultimate strategic goals for operations or wars.

A revolution in intelligence is occurring right now. Classical espionage is still in use, and one of the lessons from the post-9/11 era is the need for HUMINT. Nonetheless, the revolution which is taking place regards how new technology is changing the intelligence community.[47] Using cyber operations, intelligence services are able to penetrate and operate on a hitherto unseen scale, and classical undercover and deception operations become increasingly difficult, as big data provides the opposition with the ability to mount countermoves quickly.

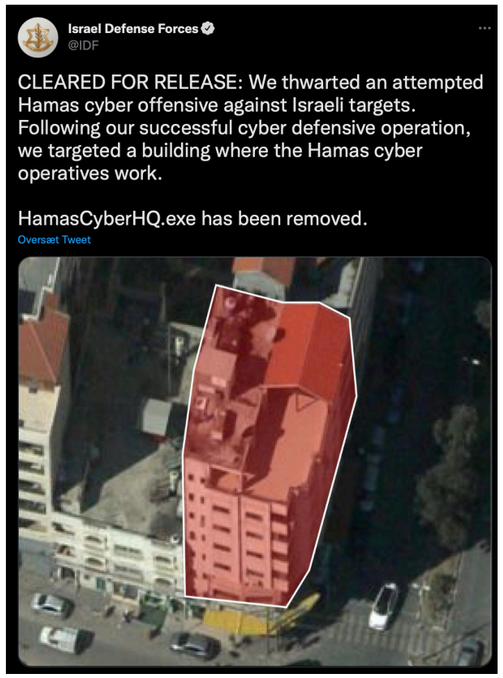
At the same time, hybrid warfare operations are constantly occurring. They are designed to take place both in peacetime and in times of war and operate on a *'phase-based scale using three separate but coordinated levels of asymmetric warfare, all of which occur during peacetime before acts of war have occurred in the grey zone.'*[48]

Jomini assumed that a declaration of war had been made and acknowledged. In his time, theoretically, there was a distinction between peace and war — a distinction that no longer exists. We must recognise that there are constant attacks targeting NATO states, their citizens, and their businesses in the cyber domain. In addition to attacks constantly occurring, it also takes a long time and requires much effort to recognise them — at least the most sophisticated attacks. Reports from private companies estimate that it takes nearly 200 days before a cyber breach has been detected and that it takes up to 69 days to contain the attack.[49]

In Chinese military thinking, the escalation ladder differs from the conception used by NATO. In China, they operate with *'stages as constituting a state of "quasi-war," and state that they have characteristics of both peace and war.'*[50] This can, at most, cause various misunderstandings and change once again by the separation of peace and war.

NATO has declared cyber as a separate domain, though in the future, it should perhaps change this to reflect the recognition of the overlap between the cyber domain, information operations, espionage, and other clandestine operations. These operations occur both in peacetime and in wartime and blur their boundaries; we must thus speak about a grey zone between peace and war. Perhaps it will help NATO understand the new battlefield to speak about the 'cyber- information and espionage domain.' It is not a succinct term, though it better demarcates the manner in which NATO ought to perceive and deal with the situation.

The challenge for NATO — and the EU — is whether or not the organisation is actually prepared to react quickly enough. The NATO Crisis Response System builds on fairly well-defined phases, yet the question must be asked whether these phases actually reflect reality. Cyber has changed the classical escalation ladder. In the 18th century, due to the necessity of gathering horses, hay, and oats, for example, the warning time could be months. At the outbreak of the First World War, a warning and subsequent mobilisation time were reduced to a matter of days or weeks. The question is whether there is a warning time at all today. Penetration of critical structures may have occurred months before an attack is carried out, and a cyberattack can be launched in seconds and cripple critical infrastructure. Is NATO actually ready for this type of extremely short warning time and the risk of extremely rapid escalation?



The Israel Defense Forces bombed Hamas as the organisation was carrying out a cyber attack. Photo Twitter/ Israel Defense Forces, @IDFDF.

DARPA's Hallmark program will provide improved capabilities to rapidly plan, assess and execute the full spectrum of U.S. military operations in space. Photo DoD graphic

Climate Photo by Sandsun / iStock-643942724

Grozny after the Russian attack. Photo Alireza numberone, CC BY-SA 4.0,

4. NEW TECHNOLOGIES – AND NEW ARMS RACES

The NATO member states need to produce state-of-the-art defence technology and equipment to secure their countries and citizens. It is crucial to understand that there is a very close connection between a strong and technologically advanced military and a strong defence industrial base. There is a need for an even stronger interaction between the military, industry, and research within NATO. American strategist Alfred T. Mahan portrayed the close connection between a strong navy, a large merchant navy, shipyards, etc., as a circular context in which the collaboration makes the individual components stronger.[51]

In 2014, the US launched the Defence Innovation Initiative, which constitutes the core of the third offset strategy.[52] The current problem is how this will be coordinated with the European powers. Seen from the outside, there is a lack of coordination, to some extent a lack of sharing, and a lack of the development of competing programs across the Atlantic. To win the technological race between NATO and all other states, NATO needs a much stronger internal competition and enhanced cooperation between research and industry. This means that not all technology shall be US-based nor European. In Europe, the European Defence Fund and the Permanent Structured Cooperation (PESCO) must be much better coordinated with NATO initiatives.

At the same time, there is a need to focus on new technology and not be blinded by the belief that technology alone can establish an upper hand in a conflict. In his 1919 analysis of tanks, Major-General J.F.C. Fuller represented this tech-fetish or fascination of weapon development. He wrote:

Tools, or weapons, if only the right ones can be discovered, form 99 per cent of victory. Strategy, command, leadership, courage, discipline, supply, organization, and all the moral and physical paraphernalia of war are as nothing to a high superiority of weapons; at most they go to form the 1 per cent, which makes the whole possible.[53]

This has been described by D.H. Lawrence, who wrote just before the outbreak of the First World War that *'science and machinery … nourish man's sense of the miraculous as magic did in the past.'*[54] In much the same way, there has been some idealisation, since at least the 1980s, about weapons with surgical precision. This was initially fuelled by the Israeli attack on the Iraqi nuclear reactor at Osirak in 1981 and later by the very well-orchestrated pictures and reports from the First Gulf War. However, precision and technological superiority are not certain and do not guarantee victory. These must be some of the harsh lessons learned from Afghanistan, Iraq, Syria, Yemen, and other contemporary battlefields.

There has always been a struggle between the defensive and the offensive. Likewise, there has always been a struggle between armour and movement. We will also see this in 2040. The medieval or contemporary discussion of armour versus mobility will find traction once more. New types of personal protection are constantly being developed. In the United States, the Institute for Soldier Nanotechnologies is advancing well, producing lighter and stronger equipment to protect the deployed soldier. A new dimension will be exoskeletons that can provide soldiers with unprecedented strength. The TALOS (Tactical Assault Light Operator Suit) is one example of this, and the comic

Nuclear explosion
Photo RomoloTavani / iStock-470309868

Cyberwarfare specialists serving with the 175th Cyberspace Operations Air Force. Photo J.M. Eddins Jr.

book Ironman may to some extent be seen as a future prospect for a Western soldier.[55]

The fascination with technology and the desire in the Western world for newer, bigger, and better weapons and weapon platforms poses a risk. Simplicity and flexibility can be lost—and with that, the possibility of winning a war. Martin van Crefeld warned against it as early as 1991 in his study of technology and war.[56] Flexibility must be a component of building new capabilities. This has been done for years in the field of naval construction. The most extreme is the Danish Standard Flex system, which makes it possible to replace individual modules and alter a unit's task from environmental monitoring to mining. Slightly less extreme is the structure of the Danish frigates, which is also based on a flexible mindset. This is repeated in the new British Type 31 general purpose frigate, and the module principle is also found in the Queen Elizabeth-class aircraft carrier.[57] A modular approach allows outdated modules to be updated with replacements as technology develops. This is known, for example, from the F-16 program, where there has been extreme development from the planes that first flew in the 1970s to the ones that fly today.

4.1 ROBOTS

Unmanned systems, or robots, represent a radical new element of the armed forces of the future. They might be unmanned, but they require humans to service them. That is to say that they are only unmanned at the sharp end. There is a large tail of humans operating the robots and servicing them. By 2040, parts of this tail may have been made smaller, and other robots may be servicing the robots. However, that requires many new technological developments.[58]

A robot is a machine with three interacting components: Sensors, processors (that can be AI) and effectors. It follows that robots can be stationary or mobile. According to the above definition of robots, drones, land-based vehicles, and certain types of artillery are all robots. A variety of technologies play a role in the development of robots. Among other things, new and lighter materials, microelectronics, energy and battery technology, combined, suggest that robots can be deployed in large quantities on future battlefields.

Robots are already deployed on the battlefield of today. The use of robots represents one of the most profound changes on the battlefield, and it has happened with astonishing speed.[59] Russia is aiming for around 30 per cent of its combat power to consist of remotely controlled and robotic platforms by 2025.[60]

The question is how many will be used in the future, whether they can operate by themselves, and whether we will allow that. In other words, the question is what the interface and interaction between man and machine will be. Robots have the great advantage that they can be deployed without the need to worry about the loss of life. They are in many ways the answer to the body bag syndrome — however, in doing so, they can also promote the use of a military solution. At the same time, one must remember that robots can be programmed to follow the rules of law, and we must consider whether robots actually will reduce the number of war crimes committed in conflicts.

The use of robots will redefine the military units. Over the next few years — until 2040 — it will be necessary to establish armed forces where robots and humans work together. The tactical and operational considerations will be reminiscent of the post-First World War considerations of the composition of armoured units and their operational deployment. In all likelihood, there will be two ways to go: Integrating the robots or letting them operate in their own groups. Integration is probably the most optimal tactical and operational approach.

Russia has, with debatable success, deployed the Uran-9 tracked unmanned combat ground vehicle in Syria.[61] Russia has created the first new formations with robot tanks.[62] However, these do not yet appear to have been tested on the battlefield in Ukraine. The vehicles are designed for fire support and reconnaissance. Little is known about their tactical deployment with Russian soldiers, though there are indications that the units are integrated. The Uran-9 is armed with a 30 mm automatic cannon, a machine gun, and M120 Ataka anti-tank guided missiles. The Uran-9 operates in a unit composed of two reconnaissance vehicles, a Uran-9 vehicle, and a command post.[63] This is the near future of war, where robots support humans. In a more distant future, they will be able to operate by themselves. At the same time, Russia is looking to use other robots for defence against missiles or drones, for example.

The lesson from history is that an armoured brigade can only to some extent operate independently and without support. When the Israeli 190th Armoured Brigade advanced in 1973, Egyptians defeated it using precision-guided weapons.[64] It is most likely similar in the case of robot armies; they may emerge as an armoured unit in a blitzkrieg scenario, but they will continue to need support and logistics provided by human beings.

Finding out how to turn a robot off becomes crucial for an adversary, be it by destroying it, switching off its systems, or taking control of it. There will be a race for this kind of knowledge in a few years. Robots are just as vulnerable to humans as are other humans and can be manipulated or turned on or off. Robots are thus not the solution to human weakness — they have weaknesses of their own.

Across the medical field, interesting research results are being published, indicating that it will be possible to equip humans with super limbs in the near future or simply to replace lost limbs. An artificial arm was developed in 2016 at John Hopkins Hospital where an electrode implanted in the patient's brain could control his fingers.[65] Projecting this forward to 2040, you will be able to have real cyborgs and, perhaps even more interestingly, develop the human brain with implants that create a superhuman. Whether this will be allowed by governments is another issue. Nonetheless, there is a real possibility that superhumans will exist or be in a late stage of development by 2040. Cyborgs, bionics, biorobots, and androids are the far future — they are certain to be actors on the battlefield in 2040. They constitute a further development and link between artificial intelligence and robots and, for cyborgs, are at the same time partly the answer to how man can maintain control over the battlefield.

4.2 ARTIFICIAL INTELLIGENCE AND AUTONOMOUS WEAPONS

Russian President Vladimir Putin observed, 'whoever becomes the leader in this sphere [artificial intelligence] will become the ruler of the world.'[66] Artificial intelligence (AI) and quantum computers represent perhaps the most ground-breaking new technology on the battlefield. Neural networking enables computers to learn to some degree.

In Chinese military thinking, we are now talking about development from a warfare where today we are 'informatised' to being 'intelligentised' in the future. This Chinese mindset seems, quite clearly, to embrace the development that AI provides.[67]

Supercomputers with a processing power equivalent to the human brain are coming in

The USAF F-117 Nighthawk, one of the key aircraft used in Operation Desert Stor. Photo Staff Sgt. Aaron Allmon II.

The Danish Frigate Absalon is build on the Flex-concept.
Photo Henning Jespersen-Skree, Flyvevåbnets Fototjeneste.

Nerekhta Unmanned Combat Ground Vehicle. Photo Militaryleak.

Turkish Bayraktar TB2 drone. Photo Army.com.ua - armyinform.com.ua, CC BY 4.0.

the next decades, and neural network computing will, by around 2040, attain something like human-level intelligence.[68] There will be a development where robots are equipped with processors with AI. It will initially be in the form of a limited capacity with clear human control, but down the line, we will leave more and more decision-making to AI, thereby reducing the reaction time.

Drones with AI are already deployed on the battlefield. Israel uses the Harpy UAV, which is launched behind the battle zone:

they loiter and search for radiating targets. The Harpy LM detects, attacks and destroys enemy radar emitters, hitting them with high hit accuracy. Harpy effectively suppresses hostile SAM and radar sites for long durations, loitering above enemy territory for hours.[69]

Thus, autonomous systems with AI are not the future — it is already on the battlefield. AI will enable *'the cognitisation of machines, creating machines that are smarter and faster than humans for narrow tasks.'*[70] It is AI that will render autonomous weapon systems so problematic and effective in the future. Currently, the new arms race consists of, among other things, a focus on autonomous weapons systems, known as 'lethal autonomous weapon systems' (LAWS). The question remains, can NATO military and civilian leadership trust machines to make life-and-death decisions in battle? The Pentagon is actually seeking to develop ethics software.[71] NATO must discuss how it will handle autonomous systems in battle. The US has a moratorium on the development of autonomous systems, which seems a high risk since Russia and China do not have such a moratorium.[72] Further, Russia and China are sabotaging the discussion in the UN of a ban on lethal autonomous weapons. In other words, NATO's possible opponents will use them.

Not ever to give up your nuclear programme must be the lesson learned from Ukraine, Libya, Syria, and Iraq. Therefore, nuclear weapons will be present in 2040, and there is a risk that even more powers will have them. As a means of blackmail, states and other actors will also focus on cheap weapons of mass destruction such as biological weapons. The crossbow was banned in 1139 by the Second Lateran Council under Pope Innocent II, though it was nonetheless employed in military action by all the European powers. The same will happen with autonomous systems. They represent such a strong potential on the battlefield that no one will abandon them and risk losing the battle. Only WMD will be weapons systems that you are considering more closely to abandon. Much of the West will be reluctant to use autonomous systems, but the risk of facing them on the battlefield will force the hope of survival and victory to bend ethical principles in the long term.

4.3 SWARM TACTICS

One of the main questions of military transformation is how tactics are changing. Right now, one of the surest changes is the emergence of swarm tactics, tactics that copy insect behaviour. Such tactics have very clear historical roots. The Mongol armies forced huge groups of prisoners in front of their regular troops to drain enemy supplies of arrows and other long-range weapons. China used massed attacks or human waves in the Korean war.[73] In the future, robots will take over these kinds of tactics, today known as swarm attacks. The Iranian armed forces have used this as a tactic for many years.[74] Swarm attacks can be carried out by an inferior actor using small but fast units and may pose a threat to larger and less flexible and thus possibly slower opponents. It is a way in which the asymmetrically inferior side can turn its inferiority into an advantage.

Drone swarm. Photo Chesky_W / iStock

On the battlefield of the future, swarms will be a tactical approach used by inferior players to paralyse a larger opponent. It could be done by deploying many, but cheap, robots and may be coordinated using AI.

Swarms are also a way of describing Western countries' network-centric operations. Swarms are resilient and flexible. *'Military swarms promise not only more adaptable and survivable forces but also new offensive and defensive tactics.'*[75] The challenge for Western military units operating in swarms is whether they will actually be allowed to operate in the partial autonomy of a swarm. Classic military hierarchy does not do well with this kind of independence, whereas it suits rebel forces or terrorists well. However, NATO forces can find inspiration in, for example, the German storm troops in the latter part of the First World War, who largely worked in a decentralised manner with tactics that resemble swarms.

4.4 MAINTAINING THE TECHNOLOGICAL EDGE IS EXPENSIVE

Normann Augustin, aerospace businessman and the US undersecretary of the Army, described in 1986 how the unit cost of a new military aircraft grows exponentially.[76] This is a problem for the Western armed forces. Professor Mikkel Vedby Rasmussen describes it as a Western military paradox: *'Why are Western armed forces achieving less and costing more?'*[77] The paradox is that nations such as the USA invest heavily in their armed forces but receive less and less in exchange for their money.[78] The situation is that the NATO states, and especially the US military, rely *"... on sustaining a qualitative edge over adversaries to maintain its combat punch."*[79] The US Congress is concerned whether potential opponents can manufacture and

The Kinzhal air-launched ballistic missile attached to a MiG-31K fighter jet. Photo: mil.ru

deploy weapons systems that are far more expensive for the United States to counter. This applies, for example, to the missile and drone domain.

Some technologies become cheaper (Louis A. Del Monte has described it as 'the Law of Decreasing Cost Returns'): *'The idea is, that as technology increase the cost of former generations of that technology decrease.'*[81] Most people know this from the purchase of cell phones. When a new model comes on the market, the older models become cheaper. In the war in Ukraine, older hand-held systems are widely used, and are crucial on the battlefield. You do not necessarily need the very latest model - as long as the older one at a cheaper price, still provides combat power. This provides unprecedented opportunities for smaller players.

Many of the wars of the first part of the 21st century were cheap wars. They were fought with cheap and light weapons, by soldiers with little or no military education and based to a large extent on civilian infrastructure.[82] This will continue. We see how smaller states or non-governmental actors use cheap, commercially available drones. For example, the Houthi movement, Ansar Allah, has made use of UAVs, which originate from the hobby industry.[83] Terrorist supporters have purchased hobby drones in Denmark.[84] In other words, it is possible that an opponent to NATO can use cheap drones/robots in lethal attacks on NATO forces.

Turkey has produced several successful drones that have now been deployed against Kurdish rebels in Turkey and not least against the Syrian forces and their Russian materiel and Russian forces in Syria. Here, the battles around Idlib, in particular, attract attention. Turkish drones and Turkish electronic warfare laid down the Syrian forces and many Russian systems. The

Turkish Bayraktar TB2 and TAI Anka seem to have defeated Russian Pantsir ground-to-air systems.[85]

The Turkish results are remarkable for at least two reasons. First, it shows that a NATO system can defeat a Russian system. The second is that Turkey developed a system by itself at a relatively low cost, a system that can match the great power of Russia This provides an insight to how, in future conflicts, smaller powers may to some extent match great powers in the deployment of drones.

Another cheap weapon is bacteria that can be easily transported. It must be considered that non-state actors or smaller states might bet on using bacteria or similar WMD in future conflicts. They are so cheap to produce and have such uncanny perspectives that an actor will at some point use them. This can be done, for example, as extortion or deterrence. This creates a need for research in the field, which fortunately will occur as a dual-purpose development.

There will be a new arms race wherein NATO must be able to handle wars involving large volumes of cheap high-tech weapons and weapon systems. The strategic impact is that robots can be used en masse against NATO. This has the potential to be a game-changer. When this same situation occurred in the past, the consequence was annihilation on an industrial scale by the deployment of machine guns and rapid-firing artillery. This could again be the answer — this time by deploying robotic counter-drone systems (counter-UAS; C-UAS). Inspiration can be found in the Counter Rocket, Artillery, and Mortar (C-RAM) systems. C-RAM has been deployed in several theatres of war and provides ground units protection against mortars, for example.[86]

Technology developed only for the military is simply too expensive for most countries. In the future, research and development must have a dual use and an interoperability dimension simultaneously. The arms race during the Cold War had a positive spill-over into the civilian sphere. Civilian and military researchers are already working together closely, though there are many opportunities to improve this engagement. Both sides must recognise that each can benefit from the other.

In this great power competition, industrial nations with strong collaborations between research, business, and defence will have a clear advantage. Universities must sacrifice some of their independence and set up security systems, including not hiring scientists from possible future hostile states. In turn, they can receive an increase in their basic research grant. The military likewise has to sacrifice some of its exclusivity. The upside for the military is that it can develop technology cheaper and maybe even of better quality. It is important that all parties acknowledge that good research is based not only on success but also on a host of failures on the path to success. Overall, it will provide society with a better return on its research and development investments.

We will see a double development where great powers will develop special and expensive weapon systems based on their technological superiority. At the same time, smaller states will use cheap publicly available technologies to disrupt and counter the much more advanced technologies of the great powers.

Within the framework of NATO — and perhaps also within the framework of the EU and future development of PESCO — the Allies will be able to focus jointly on the development of combat-critical technologies. This is reflected in NATO's work on Emerging Disruptive Technologies.

4.5 TIME, SPEED, AND RANGE

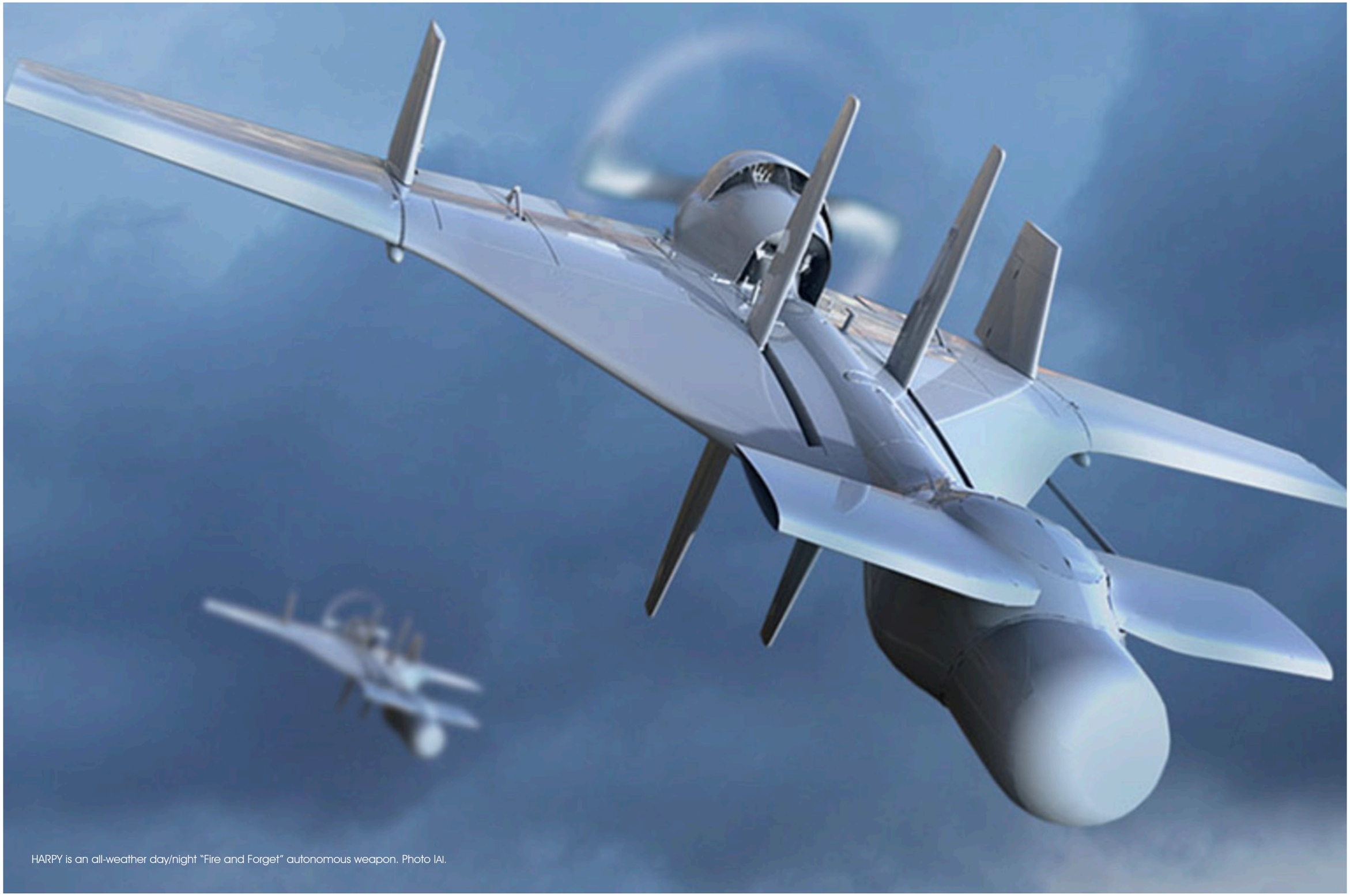
Speed is a key term when considering new technologies. Since the early 2000s, research in hypersonic weapons has been progressing.[87] Russia has already deployed Kinzhal hypersonic missiles in the war in Ukraine.[88] This means that hypersonic weapons will be implemented in the weapon arsenals within the next 10 years. Hypersonic weapons travel at a speed of over Mach 5, more than 6,000 km/h.[89]

The US Navy's experiments with railguns show that in the near future guns will be able to launch a projectile at speeds of between 7,200 km/h to 9,000 km/h.[90] Several of the great powers are conducting research and development programmes concerning long-range manoeuvrable weapons, most significantly hypersonic boost-glide systems comprising ballistic missiles equipped with hypersonic glide vehicles, and not least they can fly low and change course. Thus, they are difficult to detect and not least shoot down. These systems are extremely fast and can be used both as conventional strike capacities as well as nuclear strike capacities.[91] For Russia, the hope is that these new missile systems will be able to penetrate US and NATO missile defence systems.[92]

Hypersonic systems endanger the ability to control the escalation ladder. It is currently very difficult to track and shoot down hypersonic missiles. If an opponent uses these very fast weapons — either for conventional or nuclear capacities — it becomes more and more difficult to control a crisis.

For decades, military research and development have become accustomed to product development taking a long time. The F-35 development started back in 1992; the X-35 first flew in October 2000, and the F-35A on 15 December 2006. The first combat missions took place in 2019. In contrast, during the Second World War, it took only 102 days from the proposal and contract signing for the first P-51 aeroplane to enter the skies. Research, industry, and armed forces must find a way to develop military capabilities much faster than they currently are. There is a very high risk that you will lose the arms race if you do not establish a much faster process for developing new weapons systems.

For NATO, the increases in speed and range on the battlefield raises the question of first strike. In the future, carrier strike groups are at risk of being hit by hypersonic weapons and defeated before clear action has been taken. There is a very clear threat of a new and much more catastrophic Pearl Harbour scenario. Until now, command of the sea has been secured with seaborne platforms — and for the last 100 years, seaborne platforms with fighter aircraft — though in 2040, this might end. Command of the sea can very well be exercised with hypersonic missiles launched from land, sea, or air or by robot navies. Several countries like China and the USA are looking at developing large, unmanned surface vehicles and large unmanned undersea vehicles.



HARPY is an all-weather day/night "Fire and Forget" autonomous weapon. Photo IAI.

5. CONCLUSION

NATO's ability to adapt is historically based not only on NATO, as the organisation itself, but also on the capabilities and willingness of the member states. It must be realised that all military planning for the future is caught between prudence and paranoia.[93] Nonetheless, the political and strategy changes on a global level make it absolutely necessary that the European NATO countries realise how unfriendly the future will become and that they, therefore, invest in their military.

Europe must build military capabilities that can fight in the full military spectrum. This means that you must have tanks, artillery, frigates, and fighter jets here and now. It also means adapting to the new technologies over the next many years and incorporating them into NATO forces. However, one must not believe that there is a quick fix or that war is fundamentally changing. Many people hoped so until the Ukraine war, but it shows very clearly how new and old technology are mixed and how different types of fighting happen at the same time. We see war in cyberspace and tanks, infantry and planes deployed on the battlefield. NATO must be able to do this in the future.

Politics and strategy, as well as new technology, will in all likelihood be the strongest drivers for a military transformation within NATO. Over time, military change (the Military Revolution) has had five elements, as described above. These five elements can be used to establish a checklist for NATO's military transformation. For NATO, the following five questions could be asked to ascertain whether or not the organisation is transforming in such a manner as to fit the potential future battlefield:

1. Does NATO develop new tactics that reflect the capabilities of new technology?

2. Does the size and composition of NATO's armed forces and command structure reflect new technology and new politics?

3. Has NATO adapted new strategies corresponding to the political and technological challenges?

4. Is there an impact — or a demand — on or from society to manage the new military organisations and tasks?

5. Has NATO changed its area of operation to handle new politics and technologies such as the space or cyber domains?

These five questions were not raised in most European countries up to 1914. The political and military leaders did not reflect on or dissect the unpleasant responses they faced. If NATO and its member states are to avoid a war or, at worst, win a war, these elements must be reflected on. This must be a part of the new strategic concept.

The new escalation ladder is extremely steep; therefore, decision-making in NATO must reflect the fast-changing state of technology. At the same time, a future war will be fought in all five domains simultaneously — and there is a very clear risk that war may have broken out, and hostile acts may have been carried out long before an attack is detected. This means that NATO must establish a new command structure that can operate on a multidomain battlefield in the future.

NATO needs to focus on gaining and maintaining operational access to areas of interest to preserve freedom of action. With the changes in speed and, not least, the grey zone between peace and war, NATO must already have military capacities on high alert deployed in the possible upcoming theatre of war during peacetime.

At the same time, NATO must consider the possibility of conducting first strikes in order to maintain control over given areas. This is against NATO's identity as a defence alliance, but political clarification on the subject is needed in the near future. Technological change means that NATO must consider this course of action to survive. The combination of political and strategic change with technological change is what forces the alliance to undertake such considerations.

Similarly, NATO's political and military leadership must consider introducing autonomous weapons systems as a protection against surprise attacks. Due to the rapid escalation ladder, it is not feasible to make the necessary decisions in NATO forums before combat operations begin. This can both be a deterrent and create the necessary time for political and military decisions to be made. There is a clear risk in the future that conflicts may occur as a result of accidental or inadvertent escalation. NATO must work towards new control mechanisms that ensure that the major powers do not accidentally trigger a conflict. This means that NATO must invite globally — possibly under the auspices of the UN — for talks to create the basis for new agreements. One of the most troubling points presented in this article is the realisation that the world is facing a new arms race.

As a part of the consideration of a new political and military command structure, NATO must also consider intelligence as an independent domain in its own right. A possibility is to merge the cyber and intelligence domains into a new domain handling the perpetually ongoing intelligence, cyber, and information operations.

The technological changes will change both how we fight and the strategic spectre in which we operate. Therefore, it is important that NATO invests in research into new technologies. This can be done as an offset strategy involving all member states. It must be coordinated between NATO, the EU, and individual states. It will not be easy but is of absolute necessity.

Mass, combined with advanced technology, will be crucial to the future of the battlefield. It helps to partially alter the debate within NATO. Some states may choose to bet on, for example, many but cheap drones/robots, constituting swarms. However, it is important to adopt a broad approach so that no damaging technology monopoly occurs.

George Kennan said in a 1946 speech delivered to the National War College, '*You have no idea how much it contributes to the general politeness and pleasantness of diplomacy when you have a little quiet armed force in the background.*' This still counts — and NATO and each member country must remember it. Not just the will to show force, but also the will to use force, is a necessary component to future warfighting ambitions. This must become part of NATO's new strategic concept and in the military procurement and rearmament that each NATO member state must undertake in the coming years.

WAR IN THE FUTURE — NEW AND OLD CHALLENGES 41

7. NOTES

1. Clausewitz, Carl von: On war (ed. Michael Howard and Peter Paret, Princeton University Press, New Jersey, 1989) p. 75
2. NATO Science & Technology Organization: Science & Technology Trends 2020-2040. Exploring the S&T Edge. (NATO, Brussels, 2020) (https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf , downloaded 29/3-2022)
3. NATO: Emerging and disruptive technologies. (https://www.nato.int/cps/en/natohq/topics_184303.htm downloaded 29/3-2022)
4. Hoffman, Frank. Conflict in the 21st Century: The Rise of Hybrid War. (Potomac Institute for Policy Studies, Arlington, 2007) (https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf downloaded 29/3-2022) & John R. Schindler: 'The Coming Age of Special War' (https://20committee.wordpress.com/2013/09/20/the-coming-age-of-special-war/ downloaded 29/3-2022)
5. NATO: Remarks by NATO Secretary General Jens Stoltenberg at the Lowy Institute (Sydney) (7/9-2019) (https://www.nato.int/cps/en/natohq/opinions_168351.htm downloaded 29/3-2022)
6. NATO: good for Europe and good for America. Address to the United States Congress by NATO Secretary General Jens Stoltenberg. (3/4-2022) (https://www.nato.int/cps/en/natohq/opinions_165210.htm?selectedLocale=en downloaded 29/3-2022) &
7. Farrel, Theo & Terriff, Terry: The sources of Military Change. Culture, Politics, Technology. (Lynne Rienner Publisher, London) p. 6.
8. Johnston, Seth A.: How NATO adapts. Strategy and Organization in the Atlantic Alliance since 1950. (John Hopkins University Press, 2017)
9. Townshend, Ashley; Thomas-Noone, Brendan & Steward, Matilda: Averting Crisis: American strategy, military spending and collective defence in the Indo-Pacific. (The United States Studies Centre, University of Sydney, 2019) p. 17
10. Parker, Geoffrey: The military revolution. Military innovation and the rise of the West, 1500-1800. (Cambridge University Press, 1988)
11. Terriff, Terry : 'U.S. ideas and military change in NATO.' In Theo Farrel and Terry Terriff: The sources of Military Change. Culture, Politics, Technology. P. 111 ff.
12. Khana, Parag: The Future is Asian. Global order in the Twenty-First Century. (Weidenfeld & Nicolson, London, 2019) p. 357.
13. Kissinger, Henry: World Order. (Allen Lane, London, 2014)
14. Martin Jacques: When China rules the World. (Penguin Books, London, 2012) p. 537-538
15. Duchhardt, Heinz: Balance of Power und Pentarchie. Internationale Beziehungen 1700-1785. (Ferdinand Schöningh, Germany, 1997), p. 95ff.
16. Kennedy, Paul: The Rise and Fall of Great Powers. Economic change and military conflicts from 1500 to 2000. (Fontana Press, 1988) p. 689.
17. Milmo, Cahal: 'Insurance firms plan private navy to take on Somali pirates', in The Independent, Tuesday, 28 September 2010 (http://www.independent.co.uk/news/world/africa/insurance-firms-plan-private-navy-to-take-on-somali-pirates-2091298.html downloaded: 31/03/2022).
18. Jones, Seth G.; Doxsee, Catrina; Katz, Brian; McQueen, Eric; Moye, Joe: Russia's Corporate Soldiers. The Global Expansion of Russia's Private Military Companies. (CSIS, Washington, 2021) (https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210721_Jones_Russia%27s_Corporate_Soldiers.pdf?7fy3TGV3HqDtRKoe8vDq2J2GGVz7N586 downloaded 30/3-2022)
19. Scroxton, Alex: "Cyber companies step up support for Ukraine" in ComputerWeekly.com (02/03-2022) (https://www.computerweekly.com/news/252514063/Cyber-companies-step-up-support-for-Ukraine downloaded 30/3-2022)
20. Dixon, Patrick: Futurewise. Six Daces of Global Change. (Profilke Books, London, 2007) p. 1.
21. CSIS: Significant Cyber Incidents https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
22. Israel Defense Forces, @IDFDF: ' We thwarted an attempted Hamas cyber offensive against Israeli targets' 5/5-2019. (https://twitter.com/IDF/status/1125066395010699264 downloaded 30/3-2022)
23. Sanger, David A.: The perfect weapon. War, Sabotage, and Fear in the Cyber Age. (Crown, London, 2018), p. 216-217.
24. Defense Intelligence Agency (DIA): Challenges to security in space. (DIA, Washington, 2018).
25. Atomic Heritage Foundation: Strategic Defense Initiative (SDI) (2018) (http://www.atomicheritage.org/history/strategic-defense-initiative-sdi downloaded 30/3-2022)
26. Defense Intelligence Agency (DIA): Challenges to security in space. (DIA, Washington, 2018), p. 21.
27. Winkler; J. R.: Nexus – Strategic Communications and American Security in World War I, (Harvard University Press, 2008)
28. UN: World Urbanization Prospects. The 2018 Revision. (UN, New York, 2019) (https://population.un.org/wup/Publications/Files/WUP2018-Report.pdf downloaded 29/3-2023)
29. Spencer, John: The eight rules of urban warfare and why we must work to change them. Modern War Institute, West Point. (https://mwi.usma.edu/the-eight-rules-of-urban-warfare-and-why-we-must-work-to-change-them/ downloaded 29/3-2022) & Fox, Amos: "On Sieges" in The RUSI Journal, (2021) 166:2, 18-28,
30. Freedman, Lawrence: The future of War. (Allen Lane, London, 2017) p. 255 ff.
31. Adger, W. Neil, Juan M. Pulhin, Jon Barnett, Geoffrey D. Dabelko, Grete K., Hovelsrud, Marc Levy, Úrsula O. Spring, & Coleen H. Vogel: Human Security. In Climate Change. (Cambridge University Press, 2014)
32. Zhang, David Dian; Brecke, Peter; Lee, Harry Fung; He, Yuan-qing & Zhang, Jane: "Global climate change, war, and population decline in recent human history" in Proceedings of the National Academy of Sciences. (2007, vol. 104) (https://pdfs.semanticscholar.org/260d/512c065f8cc9f4cc7d4a7b4a40f261e2fd0d.pdf?_ga=2.203749205.499727311.1568299117-905605111.1568299117 downloaded 30/3-2022)
33. Schaar, Johan: The relationship between climate change and violent conflict. Sida working document. (SIDA, Stockholm, 2018), p. 8.
34. Lee, Harry F.: Measuring the effect of climate change on wars in history. (Asian Geographer, Vol 35, 2018)
35. Mazo Jeffrey: Climate Conflict. How global warming threatens security and what to do about it. (Routledge for IISS, London, 2010).
36. This is a bias described in economic and psychological research see Amos Tversky and Daniel Kahneman 'Judgment under Uncertainty: Heuristics and Biases' (Science, New Series, Vol. 185, No. 4157. (Sep. 27, 1974), p. 1124-1131.
37. Pettersson, Therése & Wallensteen, Peter: "Armed conflicts, 1946–2014" In Journal of Peace Research (2015, Vol. 52(4)) p. 536–550. (https://pcr.uu.se/digitalAssets/667/c_667482-l_1-k_journal-of-peace-research-2015-pettersson-536-50.pdf downloaded 29/3-2022)
38. General Knud Bartels, former NATO Chairman of the NATO Military Committee, comments to officers training, Royal Danish Defence College, 7th May 2019.

39. Rühle, Michael: 'Deterrence: what it can (and cannot) do' (NATO Review, 2015) (https://www.nato.int/docu/review/2015/Also-in-2015/deterrence-russia-military/EN/index.htm downloaded 30/3-2022)

40. Brodie, Bernard: The Absolute Weapon (New York: Harcourt, Brace, 1946) p. 76.

41. Freedman, Lawrence: Deterrence. (Polity, Cambridge, 2004) p. 116 ff.

42. Arms Control Association: Russia's Military Doctrine (https://www.armscontrol.org/act/2000-05/russias-military-doctrine downloaded 30/3-2022)

43. Oliker, Olga; Baklitskiy, Andrey: "The nuclear posture review and Tussian 'de-escalation:' a dangerous solution to a nonexistent problem." War on the Rocks (February 20, 2018) (https://warontherocks.com/2018/02/nuclear-posture-review-russian-de-escalation-dangerous-solution-nonexistent-problem/ downloaded 30%3-2022)

44. Bugos, Shannon: Putin Orders Russian Nuclear Weapons on Higher Alert. (Arms Control Association, March 2022) (https://www.armscontrol.org/act/2022-03/news/putin-orders-russian-nuclear-weapons-higher-alert downloaded 30/3-2022)

45. Amos, Jonathan: Russian anti-satellite missile test draws condemnation. (BBC, 16. March 2021) (https://www.bbc.com/news/science-environment-59299101 downloaded 30/3-2022)

46. Jomini, Antoine-Henri, Baron de: The rt of War. (Greenhill Books, London, 1992), p. 66.

47. Lucas, Edward: 'The Spycraft Revolution' in Foreign Policy (April 2019) (https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/ downloaded 30/3-2022)

48. Weissmann, Mikael: 'Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework' in Journal on Baltic Security (Volume 5 (2019): Issue 1 (June 2019) p. 19. (https://content.sciendo.com/view/journals/jobs/5/1/article-p17.xml downloaded 30/3-2022)

49. Sobers, Rob: 'Data Breach Response Times: Trends and Tips'. (https://www.varonis.com/blog/data-breach-response-times/?fbclid=IwAR00XF1p8Op1fADhN6zN8-D4O3cUNqx6pr79FgysR-liNQw6Lm8bxyxsA6gk downloaded 30/3-2022)

50. Kaufman, Alison A.; Hartnett, Daniel M.: Managing Conflict: Examining Recent PLA Writings on Escalation Control. (CNA China Studies, February 2016) (https://www.cna.org/cna_files/pdf/DRM-2015-U-009963-Final3.pdf downloaded 30/3-2022)

51. Mahan, Alfred T.: The Influence of Sea Power upon History 1660-1783. (Dover Publication, New York, 1987) p. 26 ff.

52. Hagel, Chuck (Secretary of Defense): "Memo on a new Pentagon effort to preserve the U.S. technological military edge called the Defense Innovation Initiative." (https://news.usni.org/2014/11/19/document-pentagon-innovation-initiative-memo downloaded 30/7-2022)

53. Fuller, J. F. C.: Tanks in the Great War 1914-1918. (https://www.allworldwars.com/Tanks-in-the-Great-War-1914-1918-by-John-Fuller.html#40 downloaded 30/3-2022)

54. Lawrence, D.H.: Life with a Capital L: Essays Chosen and Introduced by Geoff Dyer- (Penguin Books, London,2019).

55. Miles, Donna: Special Operations Command leads development of 'Iron Man' suit. (American Forces Press Service, 9/5-2014) (https://www.army.mil/article/125325/special_operations_command_leads_development_of_iron_man_suit downloaded 30/3-2022)

56. Crefeld Martin van: Technology and War: From 2000 BC to the Present' (The Free Press, New York, 1991), p. 282.

57. Vavasseur, Xavier: "Babcock Team 31 Selected As Preferred Bidder For UK Type 31 Frigate Programme". In Naval News (12/9- 2019) (https://www.navalnews.com/event-news/dsei-2019/2019/09/babcock-team-31-selected-as-preferred-bidder-for-uk-type-31-frigate-programme/ downloaded 30/3-2022)

58. Kott, Alexander: 'The Artificial Becomes Real" in Army ALT Magazine, Science and Technology (18/1-2018) (https://asc.army.mil/web/news-alt-jfm18-the-artificial-becomes-real/ downloaded 30/3-2022)

59. Singer, Peter W.: 'War of the Machines: A Dramatic Growth in the Military Use of Robots Brings Evolution in Their Conception.' in Scientific American (July 2010) (https://www.scientificamerican.com/article/war-of-the-machines/ downloaded 30/3-2022).

60. Eshel, Tamir: "Russian Military to Test Combat Robots in 2016" DefenceUpdate (31/12-2015) (https://defense-update.com/20151231_russian-combat-robots.html downloaded 30/3-2022)

61. Roblin, Sebastien: "Russia's Uran-9 Robot Tank Went to War in Syria (It Didn't Go Very Well)" in The National Interest. (6/1-2019) (https://nationalinterest.org/blog/buzz/russias-uran-9-robot-tank-went-war-syria-it-didnt-go-very-well-40677 downloaded 29/3-2022)

62. Saballa, Joe: "Russia Establishing First Robot Tank Unit" in TheDefencePost (13/4-2021) (https://www.thedefensepost.com/2021/04/13/russia-robot-tank-unit/ downloaded 30/3-2022)

63. Monte, Louis A. Del: Genius Weapons. Artificial Intelligence, Autonomus Weapons and the Future of Warfare. (Prometheus Books, New York, 2018), p. 187.

64. Mearsheimer, John J.: Conventional deterrence. (Cornell University Press, New York, 1983) p. 190.

65. John Hopkins Medicine (News): Mind-Controlled Prosthetic Arm Moves Individual 'Fingers. (15/2-2016) (https://www.hopkinsmedicine.org/news/media/releases/mind_controlled_prosthetic_arm_moves_individual_fingers_ (downloaded 30/3-2022)

66. CNBC: Putin: Leader in artificial intelligence will rule world. (4/9-2017) (https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html downloaded 29/3-2022)

67. Kania, Elsa B.: "Battlefield Singularity. Artificial Intelligence, Military Revolution, and China's Future Military Power." (Center for New American Security, Washington, 2017) (https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power downloaded 30/3-2022)

68. Monte, Louis A. Del: Genius Weapons. Artificial Intelligence, Autonomus Weapons and the Future of Warfare. (Prometheus Books, New York, 2018), p 109.

69. HARPY. Autonomous Weapon for All Weather (https://www.iai.co.il/p/harpy downloaded 30/3-2022)

70. Scharre, Paul: Army of none. Autonomus weapons and the future of war. (W. W. Norton & Company, 2018) p. 5.

71. Williams, Lauren C.: "The Pentagon is looking for an AI ethicist" in DefenceSystems (4/9-2019) (https://defensesystems.com/articles/2019/09/04/pentagon-ai-ethicist.aspx downloaded 30/3-2022)

72. Monte, Louis A. Del: Genius Weapons. Artificial Intelligence, Autonomus Weapons and the Future of Warfare. (Prometheus Books, New York, 2018), p. 98

73. Stewart, Richard W.: The Korean War. The Chinese Intervention. (U.S. Army Center of Military History) (https://history.army.mil/html/books/019/19-8/CMH_Pub_19-8.pdf downloaded 30/3-2022)

74. Nadimi, Farzin: Iran's Game of Drones. (The Washington Institute for Near East Policy, 2/3-

2022) (https://www.washingtoninstitute.org/policy-analysis/irans-game-drones downloaded 30/3-2022)

75. Bousquet, Antoine: The Scientific Way of Warfare. Order and Chaos on the Battlefields of Modernity. (Hurst, 2009),p. 210.

76. Normann Augustin: Augustins Laws (New York: Viking, 1986), p. 111.

77. Rasmussen, Mikkel Vedby: The Military Business. Designing Military Power for the future. (Cambridge University Press, 2015), p. 2.

78. Mikkel Vedby Rasmussen: The Military Business. Designing Military Power for the future. (Cambridge University Press, 2015), p. 254 ff.

79. Miller, James N. & O'Hanlon, Michael E.: Quality over quantity: U.S. military strategy and spending in the Trump years. (Brookings, Washington, 2019) p. 2., (https://www.brookings.edu/research/quality-over-quantity-u-s-military-strategy-and-spending-in-the-trump-years/ downloaded 30/3-2022).

80. Congressional Research Service: Navy Lasers, Railgun, and Gun-Launched Guided Projectile: Background and Issues for Congress. (CRS, Washington, 2021) (https://fas.org/sgp/crs/weapons/R44175.pdf downloaded 30/3-2022)

81. Monte, Louis A. Del: Genius Weapons. Artificial Intelligence, Autonomus Weapons and the Future of Warfare. (Prometheus Books, New York, 2018), p 106.

82. Münkler, Herfried: The new wars. (Polity Press, Cambridge, 2004) p. 74 ff.

83. Muhsin, Dhia: Houthi use of drones delivers potent message in Yemen. (IISS, 27/8-2019) (https://www.iiss.org/blogs/analysis/2019/08/houthi-uav-strategy-in-yemen downloaded 30/3-2022)

84. Dalsgaard, Louise; Vithner, Jens; Albæk, Mette Mayli & Kingo, Troels: To mænd anholdt i stor aktion: Har forbindelse til terrorsag om droner. (DR, 26/9-2018) (https://www.dr.dk/nyheder/indland/maend-anholdt-i-stor-aktion-har-forbindelse-til-terrorsag-om-droner downloaded 30/3-2022)

85. Urcosta, Ridvan Bari: "The Revolution in Drone Warfare The Lessons from the Idlib De-Escalation Zone" in European, Middle Eastern, & African Affairs (Fall, 2020) (https://media.defense.gov/2020/Aug/31/2002487583/-1/-1/1/URCOSTA.PDF downloaded 30/3-2022)

86. Holland, Arthur & Gettinger, Michel Dan: The Drone Revolution Revisited: An Assessment of Military Unmanned Systems in 2016. (The Center for the Study of the Drone at Bard College, New York, 2016) (https://dronecenter.bard.edu/files/2016/09/Report-22The-Drone-Revolution-Revisited22-.pdf downloaded 30/3-2022)

87. Congressional Research Service: Hypersonic Weapons: Background and Issues for Congress. (CSR, Washington, 2022) (https://fas.org/sgp/crs/weapons/R45811.pdf downloaded 30/3-2022)

88. Kirby, Paul: Russia claims first use of hypersonic Kinzhal missile in Ukraine. (BBC News, 19/3-2022) (https://www.bbc.com/news/world-europe-60806151 downloaded 30/3-2022)

89. Heppenheimer, T. A.: "Facing the Heat Barrier: A History of Hypersonics" in The NASA History Series (NASA, Washington, 2007)(https://history.nasa.gov/sp4232.pdf downloaded 30/3-2022)

90. Congressional Research Service: Navy Lasers, Railgun, and Gun-Launched Guided Projectile: Background and Issues for Congress. (CRS, Washington, 2021) (https://fas.org/sgp/crs/weapons/R44175.pdf downloaded 30/3-2022)

91. United Nations Office for Disarmament Affairs: Hypersonic Weapons. A Challenge and Opportunity for Strategic Arms Control. (UN, New York, 2019) (https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/02/hypersonic-weapons-study.pdf downloaded 29/3-2022)

92. Putin, Vladimir: Presidential Address to the Federal Assembly (President of Russia, ¼-2018) (http://en.kremlin.ru/events/president/news/56957 downloaded 30/3-2022) & Stone, Richard: "National pride is at stake.' Russia, China, United States race to build hypersonic weapons" In Science (8/1-2020) (https://www.science.org/content/article/national-pride-stake-russia-china-united-states-race-build-hypersonic-weapons downloaded 29/3-2022)

93. Gray, Colin S.: Strategy & Defence Planning. Meeting the Challenge of Uncertainty. (Oxford University Press, 2014) p. 191 ff.

Danish Atlantic Council
Frederiksberg Slot
Roskildevej 28 A
200 Frederiksberg
-
www.atlant.dk
atlant@atlent.dk
+45 3059 1944