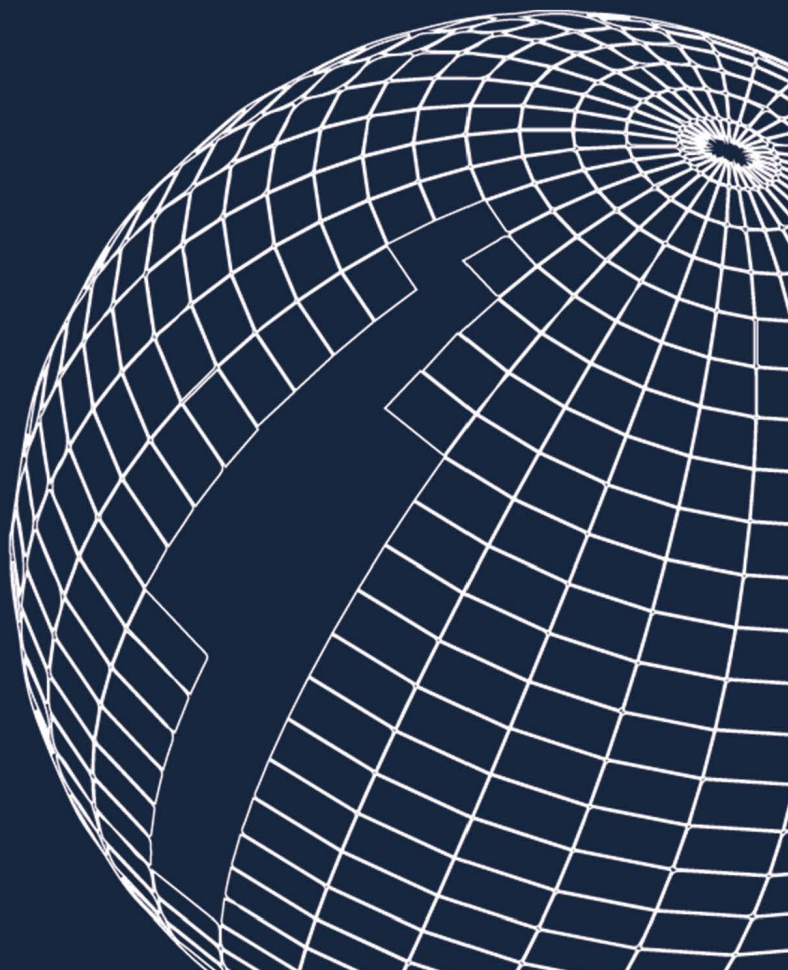
NATO Foundation
Defense College

GAME CHANGERS 2020

A new future dawns on international security



DOSSIER

The NDCF is a unique think-tank: international by design and based in Rome, due to its association with the NATO Defense College. Its added value lies in the objectives stated by its charter and in its international network.

The charter specifies that the NDCF works with the Member States of the Atlantic Alliance, its partners and the countries that have some form of co-operation with NATO. Through the Foundation the involvement of USA and Canada is more fluid than in other settings.

The Foundation was born nine years ago and is rapidly expanding its highly specific and customer-tailored activities, achieving an increasingly higher profile, also through activities dedicated to decision makers and their staff. Currently the Foundation is active in three areas: high-level events, strategic trends research and specialised decision makers' training and education.
Since it is a body with considerable freedom of action, transnational reach and cultural openness, the Foundation is developing a wider scientific and events programme.

Special thanks to PMI

NATO Foundation
Defense College

GAME CHANGERS 2020

DOSSIER

A new future dawns
on international security

NOVEMBER 2020

The Foundation wishes with this dossier,
prepared by **17 distinguished international specialists**
on **12 pivotal security subjects**, to offer a balanced and diverse
overview on topics that will change profoundly
the global strategic dynamics.

These game changers are divided into three categories:

- **emerging issues**, that are recognised as important but need a sharper focus for decision makers;
- **bridging issues**, that are already structured as a gateway to transformation in strategic affairs
- and **evolving issues**, areas that have been extensively developed since the Cold War, but that still have a great potential in the world's developments.

INDEX

EXECUTIVE SUMMARIES

EMERGING ISSUES

CLIMATE CHANGE AND ENERGY SECURITY
CHRISTIAN EGENHOFER

Climate change and the unfolding energy revolution will increasingly have a profound impact on geopolitics. For most of the 20th century, the focus of energy security has been 'uninterrupted supply' but, earlier this century, the Chinese demand shock represented a new, destabilising feature. Energy sectors will be integrated not by types of upstream products, focusing instead on location-specific competitive advantages around electricity, hydrogen or biomass.

AI AND THE TRANSATLANTIC CHALLENGE
JACOPO SCIPIONE

NATO should be a catalyst on the issue, but three roadblocks stand in the way. First, Europe sees AI mainly from an economic point of view, while for the USA it is a strategic matter. Second, for the biggest European allies the data issue represents a "battle of sovereignty": depending on the USA is a vulnerability. Third, despite China being the major adversary for Washington, the EU and NATO consider Beijing an opportunity and also a challenge.

THE PANDEMIC: SCENARIOS AND GLOBAL CONSEQUENCES
FEDERICA LOLLO AND ALESSANDRO POLITI

Pandemics and epidemics confront humanity with existential questions and represent an opportunity to rethink socio-economic and political structures and values. Governments and international organisations depend on science to take life or death choices: an unprecedented level of cooperation and solidarity is required. Unfortunately, the Covid-19 pandemic is a global stressor that has further weakened the fragile stability of the international community. It challenged the effectiveness of democratic systems; it strongly affected globalisation; and may clear the way for an economic depression and major wars.

NATO: POLITICAL CHOICES FOR DISRUPTIVE TECHNOLOGIES
BENOIT D'ABOVILLE

In the next 20 years, four emerging disruptive technologies will be crucial for the Alliance.

The proliferation of autonomous and unmanned vehicles will increase vulnerabilities for Allies in asymmetrical combat. The use of space for C4ISR, navigation and defence will remain central to many of NATO's capabilities. Hypersonic technologies may put into question the existing missile defence programmes and deterrence strategies. Quantum technologies have the potential to revolutionise operations. NATO offers proven consultative mechanisms and a unique network for collaboration on defence and security questions, being a natural platform for collaboration.

SPACE: THE LINE BETWEEN MILITARISATION AND WEAPONISATION
SORIN DUCARU

A new technological and arms race is in the offing since major countries are having as military priority the objective of limiting potential hostile operations against satellites, even if in the frame of the 1967 Outer Space Treaty's principles. As highlighted in the recent NATO space policy, space is indeed becoming an operational military domain, while the creation of Space Commands in different nations indicates an emerging concept of "space deterrence". On the other hand, in the EU space is recognized as a priority for the development of commercial services but also for its key support to security and defence where the SatCen is involved.

ENERGY SHIFTS: THE TRIPLE TRANSITION
MARCO ALBERTI

From an energy perspective, the conventional paradigm that has revolved around fossil fuels for decades is developing into a cleaner, safer model, one accessible to all. The IEA Renewables report (2019) predicts that global renewable energy capacity will grow by 50% in the 2019-24 period. This confirming that deep changes are underway. Multiple innovative technologies converge on digitised power grids, making these infrastructures crucial not only for the energy transition, but also to deliver new global political and economic structures. The old energy hubs will lose their actual leverage.

BRIDGING ISSUES

DIGITAL-SOCIAL RESILIENCE: A SHADOW GAME
ALFREDO VALLADÃO

Present-day interconnected societies, dominated by permanent and instant online divisive debates, feed the quick succession of unpredictable political "black swans", events that upset balances despite being manipulations. Apart from the universalisation of access and permanent digital innovations, "social resilience" needs an enduring participation of old representative institutions in the web of social networks. Only so one can counter authoritarian aggressions and extremist groups.

CYBER TECHNOLOGY DEVELOPMENTS AND THEIR IMPACT ON NATO
PAVEL ZUNA

In combination with other emerging technologies, Cyber Technologies (CTs) are impacting both on the present and future of security and defence. On the one hand, the complex interactions of CTs with Artificial Intelligence, quantum computing and advanced analytics will improve human decision-making abilities, reducing uncertainty and the "fog of war". On the other, CTs can be exploited perniciously for propaganda, information and psychological operations, hybrid warfare, and operations of influence.

HYBRID WARFARE AND NATO
RICHARD D. HOOKER, JR.

The Alliance is actively committed to addressing the growing threat of hybrid warfare, recognising that member states are the first and best line of defence. Allies should provide themselves with an overall strategy composed by strong cyber defence, national legislation that prohibits foreign funding of political parties, funding for counter-hybrid activities, well-integrated interagency cooperation, public information campaigns and anti-corruption programmes. NATO's public diplomacy and strategic communication should be synchronized and coordinated effectively.

NATO'S NON-MILITARY RESPONSES TO HYBRID THREATS
TEIJA TILIKAINEN

The inability to respond collectively to hybrid actors' scaled operations, which remain below the threshold of Article 5, creates serious vulnerabilities for the Alliance and its members. Alongside flexibility, collective actions against hybrid threats require the consolidation of NATO's legal resilience. The ambitious goal of NATO's non-military capacity-building against hybrid threats must be to abolish both political and legal hurdles from preventing an efficient common action. This will be also a signal of the Alliance cohesion in facing the new threats.

INFOSPHERE: THE NEED TO REVERSE A LOSING TRAJECTORY
JAKUB KALENSKÝ

The West is losing the information confrontation, while information aggressors (i.e. Russia, China and Iran) are growing in numbers and expanding the area of their disinformation activities. Focussing only on social media platforms and on the victims of the information aggression is inadequate. Western democracies should finally commit themselves in order to stop malicious actors and punish them for their malign activity.

ARE AUTONOMOUS WEAPONS ALSO INTELLIGENT?
ANTONIO MISSIROLI

The prospect of fully autonomous weapon systems has always raised serious concerns. In the past, international efforts to control the proliferation, production, development or deployment of new military technologies were all driven by four distinct but potentially overlapping rationales: ethics, legality, stability and safety. The possible military use of Artificial Intelligence, especially when related to 'standoff' weapons, has raised concerns on all four grounds.

EVOLVING ISSUES

ENERGY SECURITY
MASSIMO NICOLAZZI

In the age of energy supply abundance, the current market is further penalising the supply side through two different dynamics: the greater importers' emancipation and conversely the producers' diminishing freedom due to lower energy rents. The essence of energy security shifts from the security of supply to the protection of infrastructures, in order to secure stable and steady energy flows and to prevent outages deriving from technological or traditional menaces.

SPACE IS NOT A HIGH GROUND
BLEDDYN E. BOWEN

It is essential to avoid the intellectual red herring of space as a "high ground", because this ground is only relevant in high-intensity warfare and will be the purview only of the largest and best-funded military powers. Since the Alliance is not having its own space assets, it needs to think about a better coordination of national military space spending and capabilities. NATO's primary concern should be to build a more resilient and responsive space infrastructure.

NON-STATE ACTORS EMPOWERMENT IN THE MIDDLE-EAST
RAMI G. KHOURI

1970 is a crucial year: state-building faltered and lost credibility in the region, social conditions began to degrade, and the Muslim Brotherhood and similar groups grew impetuously. Since then Non-State Actors provided increasingly for essential personal, communal and political needs. Some NSAs grew strong and sometime shared power with

state actors for several reasons: they are anchored in the communities they serve, they are mostly uncorrupted, they speak of social justice and they emphasize equitable socio-economic development at home and confront aggression from abroad.

WEAPONS OF MASS DESTRUCTION

ERIC R. TERZUOLO

Although the Alliance is still actively engaged with arms control, non-proliferation and disarmament, there are multiple signals (i.e. the uncertain renewal of the New START Treaty) that the international community is entering a post-arms control and post-non-proliferation era. The USA's ability to exercise leadership in the Alliance will certainly be key, but NATO should focus on individual countries to promote responsible approaches and to become a relevant influencing body on the issue, although non-proliferation and arms control are not in its writ.

FOREWORD

Alessandro Minuto-Rizzo

President, NATO Defense College Foundation, Rome

International security is changing in issues, tools and balances. New threats are emerging together with new ways to deal with them: change comes in unexpected ways, unhinging old schemes and unrealistic expectations. It is not easy for the international community to grasp these realities; in other words, to connect the dots in such an unstable environment.

It is not the first time in history, but each time decision-makers have to grasp relevant aspects of the global environment in order to shape and protect the future of their communities.

Unfortunately, and perhaps not surprisingly, consensus is made difficult by different perceptions and diverging interests. And today nations uneasily connect, alongside groups and individuals that are diverging in nature and intentions. The difference from the past, is that today we know about our different counterparts much more and in shorter times: but at the same time the complexity of the overall scenario is unprecedented.

Following an established research practice, the Foundation through this Game Changers Dossier 2020 proposes short and clear analyses on different issues that have different levels of connection among themselves, trying to address what we consider to be the relevant trends, the game changers of a future that is relevant for policy making in the Alliance and in the wider international community.

We hope that an overall reflection may emerge from a collection of essays written by distinguished specialists of various nationalities. And we have the modest ambition to give a contribution, in this way, to a timely understanding of important security issues developing now and relevant for our future.

Alessandro Minuto-Rizzo

After having served at the Italian Embassy in Washington, D.C. and as Commercial Counsellor at the Embassy of Italy in Prague, Amb. Minuto-Rizzo worked as Head of the External Relations Office of the EEC from 1981 to 1986. In the next years, his career focussed on Europe and Space Policy. In 1997 he was appointed Diplomatic Counsellor of the Minister of Defence Nino Andreatta, then of his successors Carlo Scognamiglio and Sergio Mattarella. In 2000, Minuto-Rizzo held the position of Italian Ambassador to the Western European Union and to the Political and Security Committee of the EU, of which he was among the founding members. He was Deputy Secretary General of the Atlantic Alliance, between 2001 and 2007. His mandate was mostly carried out in the strategic-political industrial area, in the relations with sensitive countries such as those in the Gulf and the Southern Mediterranean. He is the author of the books: "The road to Kabul" (Il Mulino-Arel, 2009); "A political journey without maps, diversity and future in the Greater Middle East" (Rubbettino, 2013), and "NATO and the Middle East: The Making of a Partnership" (New Academia Publishing, 2018).

Emerging issues

CLIMATE CHANGE AND ENERGY SECURITY

Christian Egenhofer

Source: The New Times

Climate change is affecting more and more areas in our economies and daily life. This is no different for the military and collective security systems. Already are there signs of a 'greening of NATO' when it comes to core tasks. Climate change and the unfolding energy revolution will increasingly have a profound impact on geopolitics, going far beyond solar panels lighting our homes and powering vehicles including those used by the military.

THE ENERGY SECURITY CONTEXT IS RAPIDLY CHANGING

Traditionally the geopolitics of energy has been closely related to security. This goes back to the early 20th century with the motorization of war, starting with the UK decision to switch its navy from coal – available both domestically and abundantly across the globe – to oil. For the most of the 20th century, the focus of energy security has been 'uninterrupted supply' of energy, i.e. oil at 'affordable prices'. Earlier this century we experienced a new feature: the China demand shock. Too often it is forgotten that the US enthusiasm for a global climate change policy under President George Bush senior – leading to the adoption of the UN Framework Convention on Climate Change – has been the worry of a long-term

'unsustainable' energy demand.

The security of supply agenda has started to widen in the late 1990s, firmly including by now the security of rare earths and minor metals such as dysprosium, neodymium, praseodymium or terbium, which are required for example for wind turbines or cadmium, gallium, indium, selenium and tellurium germanium as essential parts for solar PV panels. Electricity infrastructure increasingly is being the backbone of the modern economies and defense structures.

Energy security has also become more and more influenced by the implications of global climate change and associated policies. Strong linkages to food security, water security and traditional hard security issues exist.

NEW INDUSTRIES, NEW THREATS

Whether turbines and photovoltaic panels are already on the verge of changing geopolitics forever as Adnan Z. Amin, the former Director-General of the International Renewable Energy Agency, believes, remains to be seen. Yet it is becoming increasingly evident, that climate policies will transform industrial and energy value chains.

The future energy systems will primarily be based on two energy carriers: *electricity*, produced by renewable sources, nuclear fission or possibly fusion and *hydrogen*, based on renewable energy or by using fossil fuels with carbon capture and storage or possibly pyrolysis. This will create new threats, yet also new opportunities

Biomass-based liquid and gaseous fuels will remain in the mix, albeit marginally, due to constraints of physical availability. The military may actually benefit from this.

THE NEW ENERGY GEOPOLITICS

The current 'energy space' will see a breakdown of individual energy, i.e. fuel production of natural gas or oil. Instead sectors will be integrating, focusing on location-specific competitive advantages around electricity, hydrogen or biomass.

In geopolitics, megatrends become already visible. Rents from fossil fuels erode to the advantage of energy conversion, which essentially stands for technologies, including R&D and development, trade, recycling and reprocessing of so-called structural materials such as concrete, steel, plastic, aluminum or copper alongside rare earths and minor metals.

Novel energy spaces emerge around new infrastructures, production chains and industrial clusters linked to large wind parks, low-carbon hydrogen and carbon capture and storage

infrastructure or mineral raw materials reprocessing facilities.

We should not forget about digital. A digital energy sector will be using only a fraction of fuels compared to an 'analogue' energy system, because it replaces its energy with technology. Yet at the same time, it is far more vulnerable, for example to cyber-attacks.

ENERGY SECURITY BEYOND ENERGY

It is unclear and uncertain how these long-term trends will play out. But the simple days where security of supply mainly related to 'physical availability' and 'price' are gone for good, being replaced by a more complex and uncertain world being in constant flux. The sooner policy makers accept this, the better. Or put it differently, to date energy security is not a matter for energy ministers any longer.

Christian Egenhofer

Senior Research Fellow and Director, Energy Climate House, Centre for European Policy Studies, Brussels

Senior Research Fellow & Director of CPS Energy Climate House at the Centre for European Policy Studies in Brussels, he is Adjunct Professor at the College of Europe and the Paris School of International Affairs at SciencesPo, Paris. He has been member of NATO Task Force "SAS-118 (RTG-056), Enhancing Strategic Awareness of Energy Security – A Holistic Approach".

AI AND THE TRANSATLANTIC CHALLENGE

Jacopo Scipione

Source: Shutterstock

Artificial Intelligence (AI) is a fast-developing reality and its effects will be persistent and far reaching. In its seminal forms, AI has been already used in the defence environment especially for surveillance, reconnaissance and offensive purposes by countries, private military companies, as well as by non-state actors, like ISIL, for instance in the use of off-the-shelf drones.

Despite recent debates on the actual framework in the technological race, interoperability between the European Union (EU), the North Atlantic Treaty Organization (NATO) and the United States (US) is essential to continue the cooperation among Americans and Europeans. But how interoperability could be assured if the players have a different level of technological development?

The technological gap could lead, in the long run, to the erosion of transatlantic cooperation among the two historical sides of the Alliance. Indeed, despite the EU being an economic superpower, it attracts only 8% of private investments. In addition, due to the

United Kingdom's departure, the EU may attract only 4% of investors.[1]

If the EU wants to fill this gap, European countries should invest more in the research of AI. To solve such issue, the White Paper on AI insists on the necessity to invest at least €20 billion per year for the next decade.[2] If such promises would be kept, the EU will certainly be more competitive. Particularly, related to the defence sector, the European Defence Fund and the Permanent Structured Cooperation should become the main tools to develop a stronger defence strategy on AI. Unluckily, many problems arise in relation to their nature: they both rely on the European budget that is constantly subject to pressures from member states. In this sense, the lack of pressures and constraints represents the real strength of the USA.

On the other side, NATO is facing various challenges in keeping its interoperability, because it is composed of various members that have different levels of military robustness. This could represent a strength as well as a weakness. On the one hand, NATO could benefit from the differences among countries: such divergences would increase the intra-alliance AI dependence among members, sharing decision-making processes, operations and actions related to AI.[3] On the other hand, this asymmetry could hinder the Alliance and the decisional process inside the organisation, because the US preponderance could increase frictions at defence planning and industrial level. On the operational side, US collateral damages and casualties in NATO missions could pose relevant ethical, legal and political problems regarding the use of AI by US forces. This new type of incidents could undermine the trust among allies, the effectiveness of strategic communication, the overall credibility of NATO and create political tensions.[4]

Another factor that is stirring trouble among NATO allies is the Chinese issue. Several NATO members and partners (respectively 34% and 48%)[5] are currently using and importing Chinese AI for surveillance purposes. At EU level it is well known the dispute

[1] See S. R. Soare, Digital divide? Transatlantic defence cooperation on Artificial Intelligence, European Union Institute for Security Studies, March 2020, p.5, in https://bit.ly/3kGv6KC.
[2] See European Commission, White paper on Artificial Intelligence – A European approach to excellence and trust, COM (2020) 65 final, Brussels, 19 February 2020, p.5, https://bit.ly/2HhjPSF.
[3] See S. R. Soare, Digital divide? Transatlantic defence cooperation on Artificial Intelligence, cit., p.7.
[4] See T. Valášek, "How Artificial Intelligence Could Disrupt Alliances", Carnegie Europe, 31 August 2017, https://bit.ly/3iTua5k.
[5] See S. R. Soare, Digital divide? Transatlantic defence cooperation on Artificial Intelligence, cit., p.7.

with the US concerning the Chinese presence in a future European 5G network.[6]

In a nutshell, there are three main transatlantic possible disagreements emerging on the AI issue. The first one is related to the evolution of AI and the different visions between the US and EU: while Europeans see AI exclusively from an economic point of view, the US are investing in AI in sector. The second one is linked to AI competitiveness among the two parties: for the biggest Europeans allies the data issue it is a "battle of sovereignty";[7] being vulnerable means being dependent on the US. The final issue concerns the different perception of China: while China is now the major adversary for the US administration, the EU and NATO consider Beijing a rival instead of a threat for their security.

Jacopo Scipione

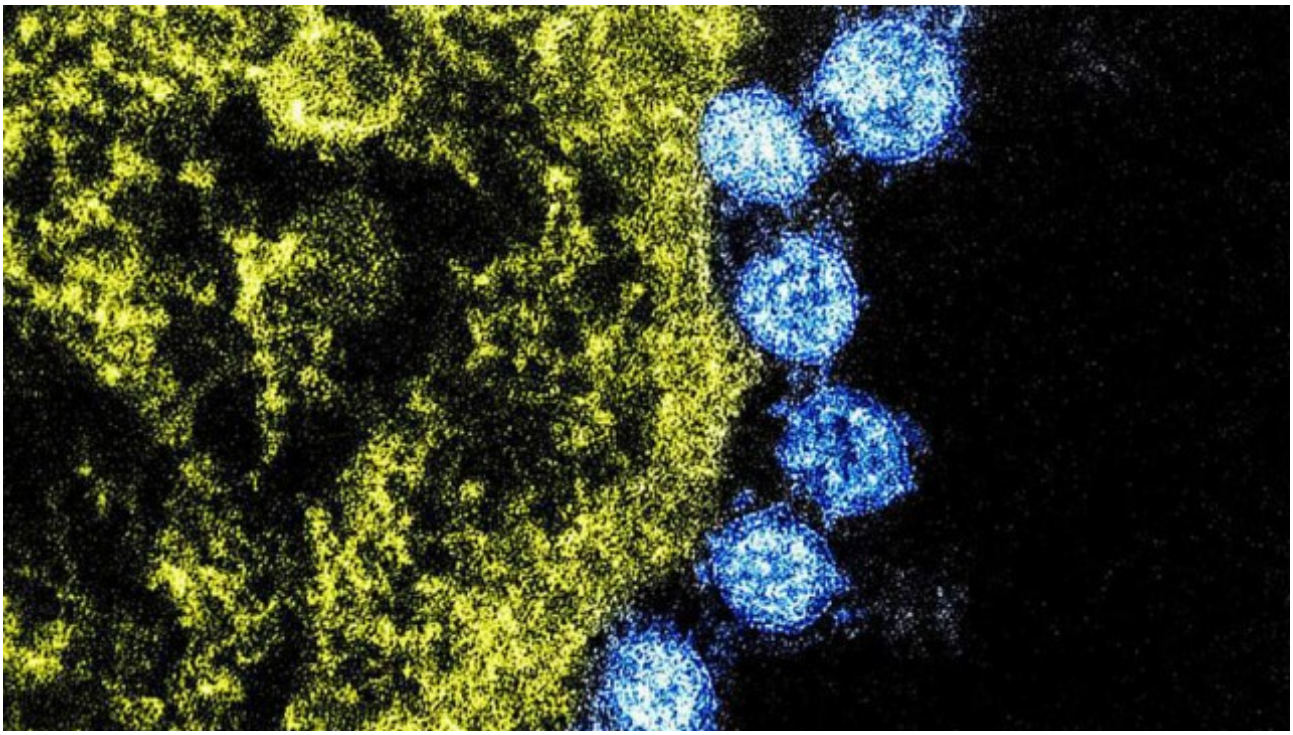
Contributor, Opinio Juris – Law and Politics Review and Geopolitica.info, Rome

A lawyer specialised in European Affairs, with a particular focus on Artificial Intelligence and the defence sector. Based in Rome, during the past year he has been Policy Officer at the Union of European Federalists. He is contributor at Opinio Juris – Law and Politics Review and Geopolitica.info. He is also part of the Executive Board of CSI – Centro Studi Internazionali.

[6] See Financial Times, US warns Europe against embracing China's 5G technology, 20 March 2020, https://on.ft.com/2Het8CS, and M.T. Esper, Speech at the Munich Security Conference, 15 February 2020, https://bit.ly/300CQiZ.
[7] See H. de Quetteville, "Emmanuel Macron's strategy to combat American data domination", The Telegraph, 18 November 2019.

THE PANDEMIC: SCENARIOS AND GLOBAL CONSEQUENCES

Federica Lollo — Alessandro Politi



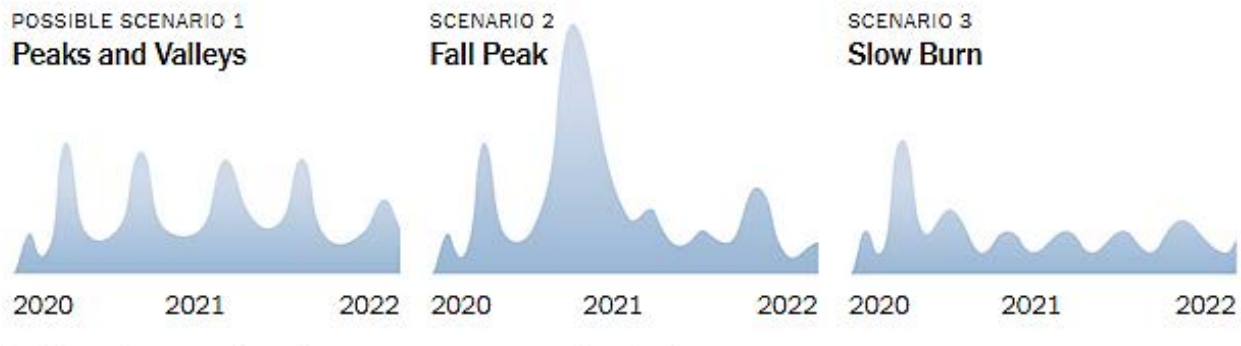
Source: Technology Networks

This short article is divided into two parts: one seeing what are the possible pandemic scenarios ahead, showing that an extensive co-operation is necessary, and the other detailing probable consequences on global balances. The final assessment is sobering beyond rhetoric calls to self-sufficiency.

PANDEMIC SCENARIOS AND GENERAL NEEDS

Pandemics and epidemics put humanity under a magnifying glass: they question our social relations with mortality, death and life. Furthermore, they open new perspectives on human interaction with the environment (both the environment that we adapted to our necessities and the natural one, responding to the previous) and on human relationships with each other's. Pandemics and epidemics shape history and could be considered like portals that give humanity the opportunity to rethink about its structure and values, and to assess its weaknesses.

The Coronavirus pandemic reminds us that we live in a so-called risk society, pervaded by a sense of an undefined but omnipresent threat that is one of the common denominators of our era. We become more and more dependent on specialised scientific knowledge to decide what is dangerous and what it is not; so, relying on science we will be defining our lifestyles and global scenarios in the long-term. Here are some possible short-term developments.



Source: The New York Times, modified from the Center for Infectious Disease Research and Policy

The Center for Infectious Disease Research and Policy, at the University of Minnesota, has developed three hypotheses on Coronavirus future waves (as in the above graph): considerable peaks and valleys diminishing over a year or two; fall or winter peaks as the common flu; and, slow burn over the years.

Whatever the outcome will be, decision-makers will have to face problems that are essential for the resilience of our societies and nations. They need to balance citizens' safety and the use of surveillance technologies to monitor the virus trends, reconciling privacy and health. Access to health services needs to be guaranteed also to the weakest sectors of populations. It will be necessary to preserve a relatively free circulation of persons at regional at regional and international level in order to prevent economic collapse.

All this requires an unprecedented level of co-operation and solidarity that by the last quarter of 2020 is still difficult to see, as it is unclear how scientific co-operation is being carried out and a fair distribution of the vaccines is planned. Despite some warnings, many governments and public opinions seem not to have fully understood neither the nature nor the wide-ranging consequences of this event.

THE NATURE OF THE EVENT

The COVID-19 pandemic must be taken for what it is: a **global stressor** (not just a stress test, but a real-life stressing agent), putting increased pressure on already very visible and vulnerable fault lines and global shaping flows.

EFFECTS ON DEMOCRACY

For the moment (25th of September 2020) some six countries seem to have managed rather well the pandemic, some despite initial serious errors and avoiding important new hotbeds: Australia, China, Finland, New Zealand, Taiwan and Singapore. Leaving aside the civilizational clash nonsense, four are democracies, one is a partial democracy and one is a single-party regime.

REPERCUSSIONS ON GLOBALISATION

Different is the outlook for the multilateral framework that underpins a still existing globalisation, particularly because political elites are often out of sync with economic realities. The response of each major government, particularly in the European Union, has been and continued to be rather uncoordinated and also NATO has had its own problems in providing a coherent response. Usually international bodies get the blame, but they have an inherently more complex decision-making process, often slowed by the biggest countries, the same that seem blandly concerned or not worried by two possible threats.

DOUBLE STORM AHEAD

Firstly, there is a strong probability of another severe financial and economic crisis in 2020 and a non-negligible possibility of a major war, if the globalisation/de-globalisation dynamics were mismanaged at the highest political level.

As the economist Nouriel Roubini correctly points out, this new crisis underway is much faster in its development by two orders of magnitude in terms of time (weeks instead of years) and much harder because it represents **a double shock on demand and supply**. If the virus diffusion is not energetically suppressed and blanket financial assistance measures are not swift enough to bridge the gap for ordinary citizens who have lost income, the serious recession risks to become a global record economic depression, dwarfing the 1929 Great Depression. As we know this depression paved the way, among other factors like resurging nationalism, weak international collaboration and democratic slides, for the Second World War.

Federica Lollo

Programme Manager, NATO Defense College Foundation, Rome

She is Programme Manager at the NATO Defense College Foundation. She worked in different international bodies such as the International Organisation of the Francophonie and the United Nations Institute for Training and Research in the Multilateral Diplomacy Programme. She collaborated on the volume "I Balcani occidentali al bivio. La NATO, KFOR e il ruolo dell'Italia" with Informazioni della Difesa.

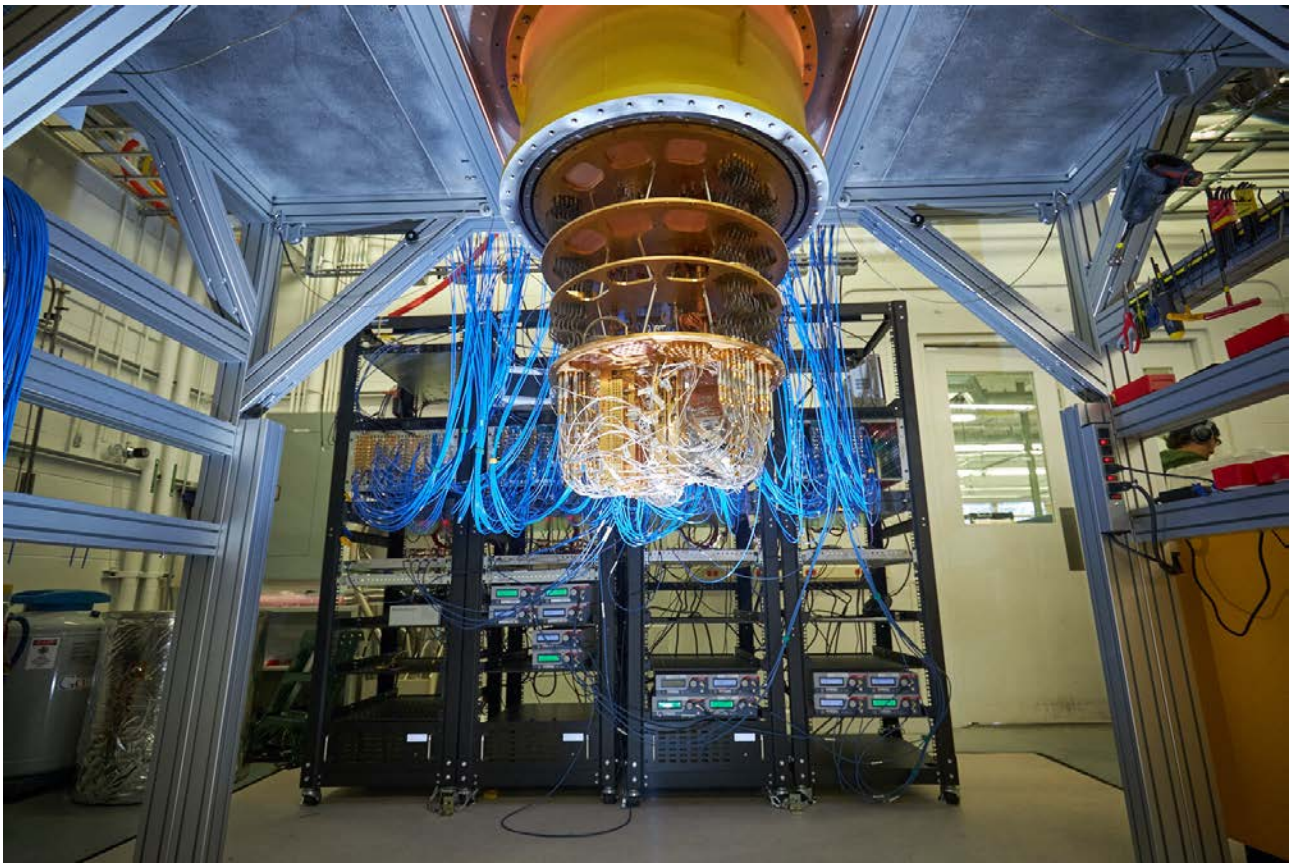
Alessandro Politi

Director, NATO Defense College Foundation, Rome

Global political and strategic analyst with 30 years of experience, he is Director of the NATO Defense College Foundation. He teaches geopolitics and intelligence at the SIOI. He was senior researcher for the Italian MoD on Latin America and global issues. He has worked with four Defence Ministers, while consulting for other three major decision makers and several governmental bodies.

NATO: POLITICAL CHOICES FOR DISRUPTIVE TECHNOLOGIES

Benoit d'Aboville



Source: phys.org

The report titled "Science & Technology Trends 2020–2040 Exploring the S&T Edge NATO", published in March 2020 by the NATO S&T Organisation (STO) is a good starting point to broach a technically complicated and politically complex debate.

The report (supported by the Alliance's defence S&T community and NATO Allied Command Transformation - ACT) points to several highly interrelated areas that are considered to be major strategic disruptors over the next 20 years: "technologies or scientific discoveries that are expected to have a major, or perhaps revolutionary, effect on NATO defence, security or enterprise functions in the period 2020-2040".

Amongst the several emerging and disruptive technologies (EDTs), either currently in the nascent stages of development or undergoing rapid revolutionary development, a few specific examples should be mentioned: data analysis, artificial intelligence (AI), autonomous vehicles, new space platforms, hypersonic missiles, quantum computer

technologies, biotechnology used for defence, and new materials.

These are at different stages of development. Data, AI, autonomy, space and hypersonics are already in use and are seen to be predominantly disruptive in nature, as developments in these areas build upon long histories of supporting technological development. As such, a significant or revolutionary disruption of military capabilities is either already ongoing or will have a significant impact over the next 5–10 years.

New developments in quantum, biotechnology and materials are assessed as being emergent, requiring significantly more time, 10–20 years, before their disruptive natures are fully felt on military capabilities.

Amongst the full list of the technologies named in the report, four EDTs seem to be especially worth considering, if only because they are already a current priority for many allies at the national level.

Autonomy and unmanned vehicles are already widely in operational use in allied operations, but their proliferation (e.g. cheap drones in Syria and Libya) increase vulnerabilities for allies in asymmetrical combat and can be used in swarms to clear the way for penetration of strike aircraft in air defence systems, supplanting the old Wild Weasel tactics.

The use of space for C4ISR, navigation and defence is central to many of NATO's existing capabilities, and ultimately it is the foundation upon which NATO has built a technological edge. In the next 20 years this will imply increasingly capable and ubiquitous C4ISR capabilities and the combination with AI will be synergetic. On the other hand, risks from ASAT (anti-satellite) or robotic parasitic systems will become more acute. More congested orbits, the increased use of large constellations of small satellites and increasing levels of space debris will impact the effectiveness and reliability of space-based systems, impairing the Alliance capabilities.

Hypersonic technologies applied to rocket, scramjet or combined cycle propulsion systems, are now considered a priority in the USA, China and Russia, as well as by Japan, France, the UK, India and Australia. This class of weapon system includes air-launched strike missiles (HCM, Hypersonic cruise missiles), manoeuvring re-entry glide vehicles (HGV, Hypersonic glide vehicles), land-sea ship killers, and post-stealth strike aircraft.

Countermeasures against individual, salvo or swarm hypersonic systems are particularly challenging due to their speed and manoeuvrability. To what degree this puts into question the existing missile defence programmes and the existing decision cycles of deterrence are essential debates that should, sooner or later, be opened within the Alliance.

Although new quantum technologies have the potential for a revolutionary impact on NATO operations, most (but not all) are in the early stages of development, and significant technical challenges lie ahead before operational systems can be developed. The use of ultra-sensitive gravimetric, magnetic or acoustic sensors will significantly increase the effectiveness of underwater warfare capabilities, potentially rendering the oceans transparent. Quantum technologies have the potential to make stealth technologies obsolete, provide more accurate target identification, and allow covert detection and surveillance. Accurate clocks will enable the development of (precision) positioning, as well as precision navigation and timing (PNT) systems for use in GPS-denied or inaccessible areas (such as under-ice). Unbreakable quantum key encryption will support substantially more robust and secure communication. Quantum computing, potentially the most disruptive quantum technology of all, has the potential to render previously untenable classical computational tasks.

Some of the conclusions of the NATO STO study are worth quoting in full:
"[The] productive employment of these new technologies will pose severe challenges and raise fundamental questions of ethics and legality. [...] Information itself will increasingly become a warfighting domain and a commodity. In parallel, the use of automated and potentially autonomous systems in operations in which humans are not directly involved in the decision cycle, will become more widespread and increase the pace of strategic competition".

"While it is likely that the Alliance will maintain a degree of technological advantage in some EDT areas, EDTs (in particular AI, Big Data, biotechnology, hypersonic) will likely become cheaper and more accessible to hostile actors. The Alliance's dependence on advanced technology could increasingly become a liability if care is not taken on how they are integrated and in the development of counter-measures. ... It is essential that we understand the nature of these new technologies, analyze their implications for defence and security, explore the opportunities they offer, push the boundaries of what is possible, and ensure that we are ready to mitigate their risks. NATO is by its international and collaborative nature well placed to consider these issues".

NATO offers proven consultative mechanisms and a unique network for collaboration on defence and security questions, being a natural platform for collaboration. Other proposed format like "techno-democracies" might prove more difficult to manage than expected.

But for such a debate to be productive, one has first to convince the decision makers and the public in the Alliance that these technologies applied to defence have an increasing momentum on their own, and, if we want to redirect it towards our own security interests (or convince others that there is a potential shared interest through arms control), we cannot be complacent or ignore facts. Denying ourselves these capabilities will not stop potential adversaries in pursuing them for their own interests.

Benoit d'Aboville

Vice-President, Fondation pour la Recherche Stratégique, Paris

A former career diplomat, Ambassador d'Aboville served as Permanent Representative to NATO (2000-2005) and Senior Auditor at the French National Audit Court (2005-2011). During his diplomatic career, he has been posted in Washington, Moscow, Geneva, Madrid (CSCE) and New York. Since 2014, he is Vice-President of the Fondation pour la Recherche Stratégique in Paris.

SPACE: THE LINE BETWEEN MILITARISATION AND WEAPONISATION

Sorin Ducaru

Source: Shutterstock

About 2.400 operational spacecrafts are currently in orbit, a number expected to increase by up to 10 times over the next years due to the deployment of large constellations of satellites. Indeed, space assets are more and more vital for our digital society and both private and governmental users are heavily investing in space to provide key advantages compared to other commercial competitors or nations. A sustainable space environment is therefore essential for the exploitation of the associated services while two aspects clearly threaten its guaranteed open use.

Firstly, the space debris are today noted as worrying while in future their number, following the trend of deployed satellites, will be a huge challenge to cope with on some Low Earth Orbits (LEO): the current procedures used to avoid collisions, based on phone calls and mails, will have to be largely improved and today the concept of space traffic management is thus emerging. The "Guidelines for the Long-term Sustainability of Outer Space Activities", approved by the UN Committee on the Peaceful Uses of Outer Space in June 2019, represent a first milestone towards a rule-based system.

The EU's initiative for Safety, Security and Sustainability of Outer Space (3SOS), as

presented in September 2019 at the Earth Observation Summit in Paris, by Carine Claeys, Special Envoy for Space, aims at developing a sustainable space environment while the EU Space Surveillance & Tracking program is the first European operational step. To support this change of paradigm, large investments will be required to improve space situational awareness, particularly surveillance and tracking. Since space is a common good, an international approach is needed and cooperation in that field is a must.

Secondly, space technologies are supporting both civilian and military activities. They are inherently dual use. Space capabilities contribute to defence information superiority and enable other military assets in providing services for intelligence, reconnaissance, communication, timing and positioning. The increasing use of space assets to support security and defence objectives, including military functions, has led to the use of term such as "space militarisation".

Conceptual clarity is important, however. Militarisation is different from weaponisation of space.

The first concept refers to supporting military activities (just as civilian ones) through telecommunications, geo-location and earth observation based on space capabilities. It has been an important function from the early days of space technological development, very much like the use of other new technologies as military enablers. Military weapons are the ones aim at achieving the operational effects. Therefore, "space weaponisation" would be indeed a game changer, since it points to achieving direct military operational effects through space capabilities.

Whereas the use of space assets to support and safeguard national strategic interests and military enabling functions is essentially unavoidable and in line with enabling functions of other technologies, the weaponization of space is quite another dimension, which cannot be excluded from any strategic foresight study but with some important (and potentially strategic) consequences that need to be thoroughly analysed and addressed.

Numerous examples of spoofing, jamming or laser dazzling of telecom or navigation and positioning satellites show the dangers of space abuse. Evolving technologies, such as orbit rendezvous can be exploited to approach a satellite and spy on it, or even damage its functionality. Thus, limiting potential hostile operations against satellites is becoming a military objective, while staying in the frame of the 1967 Outer Space Treaty's principles.

As a consequence, the protection and defence of satellites is also becoming a priority, opening the way to a new field for an arms race. It is interesting to note that the creation of Space Commands in some space faring nations, but not only, is demonstrating the emerging concept of "space deterrence". Space is indeed becoming an operational military domain, as the recent NATO space policy highlights.

In conclusion, the space domain is increasingly competitive and the need to use it for civil and military applications is an exponential trend. Space is also becoming more congested and contested, potentially limiting its future use. The balance between these two aspects will greatly depend on the cooperation between nations as well as public and private actors, but also on the allocated financial resources to develop and operate the needed technologies ensuring the free use of space.

The EU Satellite Centre (SatCen) in Torrejon Madrid, which I have the honour to lead, has a dual enabling function:

- The core function is that of providing "security from Space" to Earth, through its highly responsive, adaptive and valued geospatial intelligence focused activity.
- SatCen is also providing "security for/in Space", acting as service front desk and user interface within the EU Space Surveillance & Tracking program, aimed to evolve towards Space Situational Awareness. Both functions are based on cutting edge technology.

In the EU, space is recognized as a priority for both, the development of commercial services but also for its key support to security and defence where SatCen is involved. Indeed, the next Multiannual Financial Framework will increase the budget allocated to the civil EU Space Program while the new **European Defence Fund** will support the military Member States cooperative developments, including in space. These financial perspectives are also important for the SatCen future, the only autonomous, operational geo-intelligence institution of EU that supports the Common Foreign and Security Policy as well as Members States.

Sorin Ducaru

Director, European Union Satellite Centre, Madrid

Since 2019, Ambassador Sorin Ducaru is the Director of the European Union Satellite Centre. He held the post of NATO Assistant Secretary General for Emerging Security Challenges. He also served as Romania's ambassador to NATO, the USA and the United Nations.

ENERGY SHIFTS: THE TRIPLE TRANSITION

Marco Alberti

Source: unicreditgroup.eu

No time of transition is completely linear. The one we are facing is even less so, characterised as it is by the simultaneous action of three intertwined transitions. The energy transition, the digital transformation and a general re-balance of global power, with a possible regionalisation of international affairs. Given their high speed, these transitions create remarkable opportunities, but they also produce significant systemic discontinuities. A different mind-set, as well as new conceptual and operational tools, are therefore required to deal with circumstances that are every time less predictable and often characterised by highly destabilising phenomena, as seen in the COVID-19 outbreak.

From an energy perspective, the conventional paradigm that has revolved around fossil fuels for decades is developing into a cleaner, safer model, one accessible to all. The Bloomberg New Energy Outlook 2018 estimates that, by 2050, almost 50% of electricity worldwide will be generated by renewable sources. Meanwhile, the IEA Renewables report (2019) predicts that global renewable energy capacity will grow by 50% in the 2019-24 period. These forecasts confirm that deep changes are ongoing.

In some ways, every energy transition is the result of accelerations in technology and has political, economic and social impacts. Change is underway regarding infrastructure, markets, benchmark resources, stakeholders and strategies, socio-technical regulations and consequently also in the geopolitical balance of power. The same has occurred in the transition from wood to coal, then in turn from coal to oil and gas. Something similar is happening even now with renewables, based on a decentralised, digitised and sustainable production-consumption paradigm. It will certainly not be a sudden shift. We will experience a period of transition, during which the geopolitics of hydrocarbons and of renewable energies will be required to co-exist, sometimes complementing each other, overlapping at other times.

During the transitional phase, policymakers must assume responsibility for taking their countries towards new, sustainable models, by ensuring that the energy transition is ***fair*** including from a geopolitical perspective. In other words, they must prevent the energy paradigm shift from evolving into a cause of socio-political destabilisation. Moving in this direction requires an anticipatory vision of the changes and new strategies, suited to the rapidly evolving concept of energy security. Furthermore, massive injections of innovation will be necessary to fully exploit the huge potential of the new energy paradigm.
Digitisation is redrafting the "map" of modernity and, with it, the stratification of power and the rules that governing power. The new paradigm will focus on electrification and will thus lead to further digitisation of the system. The geopolitics of energy, to date intricately linked to the geographical concentration of hydrocarbons and the delicate issues of their transportation, will need to deal with new and decisive aspects, such as cyber security, the supply of critical materials and the control of new technologies that have an increasing influence on countries' energy security and policy.

Renewables are recasting the structural nexus on which the geopolitics of hydrocarbons is based: abundance/scarcity, dependence/security, stability/fragility. The relationship between energy security and the re-distribution of global power persists, although in a different perspective. While energy remains one of the cornerstones of geopolitics, certain natural resources, although contested, will be no longer so scarce as to allow to be used as instruments of influence, pressure or deterrence. Multiple innovative technologies converge on digitised power grids, making these infrastructures a crucial hub not only for the energy transition, but also to deliver new global political and economic structures.

Even in the energy sector, the confrontation (or cooperation) among sovereign powers will

be principally technological, and in the future, geopolitics will be "functional" to the development of infrastructure connectivity. We are moving towards a new representation of global power and its balance. Ultimately, no energy transition has ever remained completely isolated from geopolitics. Nor will the present one. The first countries to realise the change by adapting their strategies, whether national or business, are likely to become successful leaders in the energy transition.

If we want to help in consolidating energy security and match it with the evolution of the current paradigm, we have means to invest in the political and institutional stability of countries and in the prosperity of their populations. Tackling the triple transition is an urgent global challenge, one from which we cannot escape.

Marco Alberti

Head, International Institutional Affairs, Enel, Rome

Acting as Head of the International Institutional Affairs, he coordinates Enel Group's global public affairs activities and supports the Business Lines in international development. He also collaborates with the Strategic Unit on geopolitical and geo-economic issues. His activity is focussed on energy transition, climate change, and State-to-city diplomacy.

Bridging issues

DIGITAL-SOCIAL RESILIENCE: A SHADOW GAME

Alfredo Valladão

Source: surfincloud.com

"Social resilience" is a much uncertain concept. How and who defines the social compound that should be protected in order to survive the threats that can destroy it? Social resilience implies political decision processes led by an authority powerful or legitimate enough to prevent – and deliver "solutions" – to perceived challenges.

But human societies – even in their most primitive or totalitarian forms – are not monolithic blocs. There is no whole consensus about what should be "resilient" and what threats should be prioritized. Decision-makers can only hope to express a majority view in their circumscribed constituencies. Their policy-making rests on a combination of persuasion and constraints that inevitably produce winners and losers. But an old question lingers: are they just trying to "save" (or maintain) their own "establishment" and social power-basis or are they working for the "common good"?

Then, resilience also requires grading possible preventable threats. Known or unknown challenges are infinite, but resources are not. A successful national resilience program

always sacrifices the interests of some categories of citizens or regions inside a country and can be perceived as detrimental by neighbouring States or the international community. Prohibiting exports of medical equipment by member countries did not, for instance, help a common European Union response to the COVID-19 epidemic.

These classical predicaments of any political body have been drowned into the pervasiveness of social media and the Internet. Hyper-connection without borders, allowing any small group (even a single individual) to sometime exert a disproportionate influence (worldwide and in its own community) has deeply undermined the authority and legitimacy of standard social-political institutions. Governments, political parties, trade unions, electoral or judicial systems, and even traditional religious denominations, have often lost control over social narratives.

Greta Thunberg or a smartphone video – captured by a nineteen-year old – showing the atrocious assassination of a black man by a police officer in Minneapolis, have the power to mobilize hearts and minds of masses of people all over the planet. It means imposing straight off new issues and agendas upon decision-makers and political institutions everywhere. The different answers to the global coronavirus pandemic have been so shredded apart by social media that they became hopelessly politicized inside and between national States; thus, undermining the representativeness of political and social institutions (local, national and international) and, more ominous, the simple pursuit of truth by scientific and medical establishments.

Present-day interconnected societies, dominated by permanent and instant online divisive debates and opinions, feed the quick succession of mostly unpredictable political "black swans". Many prevention policies resemble generals re-fighting the last war. Decision-makers are compelled to supply rapid responses to decisive challenges they didn't see coming. In this indefinite environment, "social resilience" strategies have to be based either on authoritarian or freedom values.

Disinventing the Internet is not an option because cutting access to the net can be a short-time solution, but self-defeating in the long run. On the one hand, authoritarian regimes are learning to use the new digital technologies in order to impose a totalitarian control over their "societies". On the other hand, those who treasure individual freedoms, democracy and rule of law will have to learn how to devise proactive policies adapted to the new social cyberspace. In a networked world, disruption can spread quickly, but the

disruptive effects can also be diluted by the shear complexity of the net.

Today, promoting "resilience" based on freedom implies favouring a fast universalization of access to interconnectedness, as well as decentralized and permanent innovations in the field of digital technologies. But "democratic" resilience also needs serious overhauling and transformation of old representative institutions through an enduring participation in the web of social networks, in order to counter big players' authoritarian aggression, as well as toxic individuals and extremist groups that threaten social cohesion. This responsibility certainly lies on the decision-makers shoulders, but also on all civil societies' line-ups and single persons who are ready to take sides on this new replay of the traditional confrontation between dictatorship and freedom.

Alfredo Valladão

Professor, Paris School of International Affairs, Science Po, Paris

He is a Professor at the Paris School of International Affairs, Sciences Po, where he acted as Director of the Mercosur Chair from 1999 to 2010. He is also President of the Advisory Board of EU Brazil Association, Brussels. In addition, Professor Valladão is Senior Research Fellow at the Policy Center for the New South, Rabat.

CYBER TECHNOLOGY DEVELOPMENTS AND THEIR IMPACT ON NATO

Pavel Zuna

Source: cybertalk.org

Since the Wales Summit in 2014, NATO has adopted a Cyber Defense Policy and recognized Cyber Space as a domain of operations in which the Alliance must defend itself as effectively as in other domains of operations.

Cyber Technologies (CTs) are advancing in the cyberspace of the virtual computer world, particularly within the electronic medium used, to form a global computer network to facilitate online communication, data exchange, and processing activities.[8]

As we talk about "Cyber Defence" and the ability of our Allies and partners to defend themselves in this domain, we need to ask whether CTs belong to the important game changers within NATO's collective defence, crisis management, and cooperative security.

[8] Cyberspace. Technopedia [online]. Techopedia, 2019 [cit. 2020-6-4]. Available at: https://www.techopedia.com/ definition/2493/cyberspace.

Assessing where and how CTs will impact NATO's core missions, we need to first go back to the basics of armed conflicts. As Clausewitz and J.F.C. Fuller described, armed conflicts are governed by a trinity of dialectical relations between mental, moral and physical elements of the belligerents' strengths at all levels of conflict.

What then is the impact of cyber technologies on those strengths? Do CTs completely change how belligerents will influence and exploit these elements efficiently under the law of the economy of force, or do they provide just another tool to achieve a desired effect?

From the short- and mid-term perspective, a combination of complex interactions of CTs with Artificial Intelligence, quantum computing, and advanced analytics will significantly affect the mental elements of strength in conflict. Because human cognitive and decision-making abilities are limited by genetic and cultural heritage, as well as education and experience, when AI is applied through CTs and quantum computing, those human limitations can be overcome. That augmentation of the human cognitive aspect will have fundamental impacts, promising to reduce uncertainty and the "fog of war".

The moral element of belligerent strength, in other words the will and determination of nations, decision-makers, commanders, and soldiers to wage and conduct armed conflict, has been the target of belligerents for centuries. We talk frequently about propaganda, information and psychological operations, hybrid warfare, and operations for influence etc.; however, CTs can be used effectively for that purpose. Again, with the application of AI and quantum computing, social media, along with the evolution of the new, automatic computing algorithms, the human cognitive domain is going to be exposed to the manipulation, disinformation, and data gathering for intelligence purposes. In that sense CTs, in combination with other emerging technologies, will not bring revolutionary change, but a rather significant evolutional impact.

There is no need to elaborate on CTs' impact on the physical elements of belligerents' strengths as this is very broad topic stemming from national economies, critical infrastructure down to weapon systems, C3 systems etc. CTs are already applied through the systems of systems and the evolution goes further towards interconnectedness and distribution across all domains to include land, sea, air, space, cyber, and information. What we can expect in future will be interconnectedness with human cognitive domain: the end result will be that humans will be able to exploit huge data to orient, decide, and

collaborate anywhere and anytime.

CTs, by themselves, are neither disruptive nor revolutionary game changers. However, they impact and will continue to impact current and future security and defence significantly in an evolutionary manner and in combination with other emerging and evolving technologies.

NATO Science & Technology Trends Report identifies four developing strategic S&T trends with potential game changing roles: intelligent, interconnected, distributed and digital[9]. Those four trends will inevitably shape future exploitations of the CTs for defence.

Pavel Zuna

Director, NATO Science & Technology Organization Collaboration Support Office, Neuilly sur Seine

Director of NATO STO Collaboration Support Office in Neuilly-sur-Seine. He is a retired Colonel with a 30-year active military service career. He retired as Deputy Director of the Military Counter-Intelligence and Military Intelligence Service and served as Assistant Defence Attaché to Belgium and Defence Attaché to the United Kingdom.

[9] NATO Science & Technology Organization. *Science & Technology Trends 2020 - 2040: Exploring the S&T Edge* [online]. Brussels: NATO Headquarters, 2020, 160 s. [cit. 2020-6-4]. Available at: https://www.sto.nato.int/pages/tech-trends.aspx

HYBRID WARFARE AND NATO

Richard D. Hooker, Jr.

Source: strategyinternational.org

As NATO contemplates a new Strategic Concept, hybrid warfare will assume an important role in the Alliance thinking and planning. Though not new, this form of confrontation is both dangerous and effective, undermining Alliance unity and cohesion and eroding the very basis of collective security. Meeting this challenge requires both a shared understanding of its nature, and the political will to address and counter its many different manifestations.

Though the definitions applied to hybrid warfare differ slightly, in general the term refers to conflict in the information domain, below the kinetic level. Subversion, propaganda, deception operations, disinformation and offensive cyber operations are its hallmarks. Penetration of Alliance intelligence services, suborning government officials, financing nationalist political parties and covert interference in democratic elections are common manifestations. Cyber-attacks that affect targeted economies and national media – particularly social media platforms – can be especially damaging. Though non-state actors such as ISIS may employ hybrid approaches, the most dangerous threats emanate from powerful state sponsors. Above all, the Russian Federation fields the most capable set of

tools and organizations operating against NATO members in this domain.

Hybrid approaches employed by Russia have deep roots in the Soviet and even Czarist eras and can be applied seamlessly with the more formal military, economic and diplomatic instruments of power. Russia benefits from a centralized, top down system of political organization that is more coherent and less bureaucratic than western democracies. A lack of transparency and the deliberate use of surrogates, such as unmarked paramilitaries, private security contractors, ethnic Russian parties in foreign countries and internet trolls, give an opaque aspect to what is clearly a state-sponsored and state-directed activity. The purpose is to sow doubt and distrust in targeted capitals and societies and to disrupt and degrade their political communities. In this way, Russia shapes the security landscape in its favour and in consonance with its long-term objectives.

In recent years, the Alliance has taken note of the growing threat of hybrid warfare and moved to address it. NATO's strategy for countering hybrid warfare appropriately recognizes that member states are the first and best line of defence. NATO doctrine and staff expertise, Counter-Hybrid Support Teams and Centers of Excellence for Cyber Defense and Strategic Communications help to build resilience into the Alliance. Many allies have reorganized their government structures to cope with cyber intrusions and attacks more effectively. There is growing awareness of the nature of the threat and its potency. These first steps are important and meaningful, but much remains to be done.

An inherent difficulty is that many of the institutions that once combated Soviet disinformation were eliminated at the end of the Cold War. The U.S. Information Agency, for example, played a critical and successful role, contributing decisively to the outcome. For some years following its disestablishment, the U.S. government neglected the information domain. Today, almost two dozen separate functions related to countering adversary disinformation and hybrid warfare are distributed among scores of government offices. The lack of a unified and well-coordinated mechanism tying these functions together is a serious problem. Many allies suffer from similar disabilities.

In other cases, the openness and transparency of democratic institutions – the very strength of the Alliance – can inhibit effective responses. For example, covert intelligence activities will often be required to combat hybrid warfare, while specific capabilities such as offensive cyber must remain highly classified to be effective. Here, Allies must strike the

right balance between national security and civil liberties, preserving core values while retaining the ability to compete against a resourceful and capable adversary.

To improve performance in countering hybrid threats, Allies can and should consider discrete steps focused on the threat. Strong cyber defence, national legislation that prohibits foreign funding of political parties, well-integrated interagency cooperation, funding for counter-hybrid activities, public information campaigns and anti-corruption programs are all component parts of an overall counter-hybrid strategy. Public diplomacy and strategic communication in capitals and at NATO headquarters should be synchronized and coordinated.

NATO has already taken the first and most important step. Awareness of the challenge, its nature and the threat it poses to Alliance unity and cohesion, is well advanced. NATO also competes from a position of strength: its democratic institutions, respect for individual rights and liberties, and opportunities for economic success and social mobility undergird and support a winning narrative no adversary can match. Building on these strengths, NATO is well postured to compete and prevail.

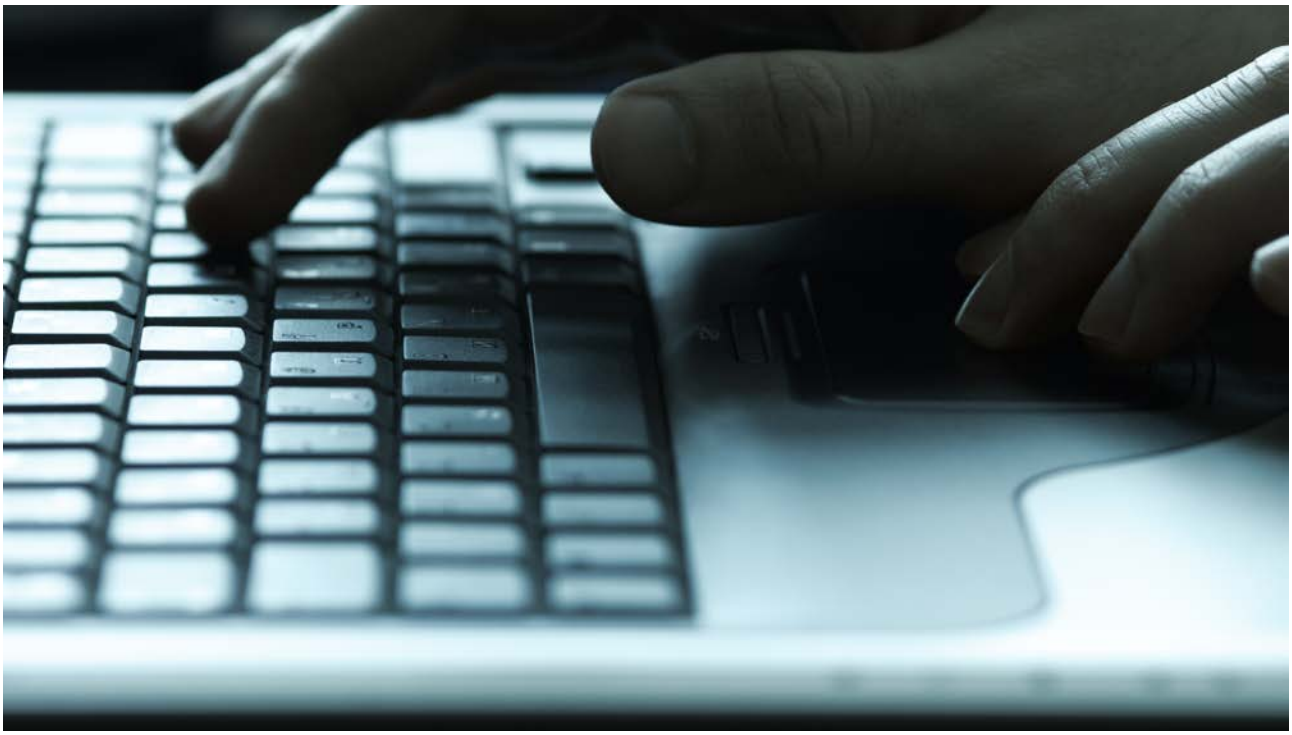
Richard D. Hooker, Jr.

Former Professor, National War College, Washington D.C.

Former Colonel of the US Army, Dr Hooker joined the National War College in 2018 after previous service as National Defense University's Director, Institute for National Strategic Studies (INSS). He previously served as Assistant Professor at West Point, as the Army Chair at the National War College and as Dean of the NATO Defense College in Rome.

NATO'S NON-MILITARY RESPONSES TO HYBRID THREATS

Teija Tiilikainen



Source: Shutterstock

Hybrid threats refer to political power being exerted in a very specific form in international politics. As exertion of power in general, hybrid actions aim at affecting the target state's decision-making to the benefit of the acting state or non-state actor. Hybrid action is characterized by the use of unconventional means trying to take advantage of the vulnerabilities of the target state or collective actor such as the EU or NATO. Disinformation and interference in political debate or elections, critical infrastructure disturbances or attacks, cyber operations, different forms of criminal activities and, finally, an asymmetric use of military means and warfare, belong to typical forms of hybrid action.

By using a set of aforementioned unconventional means in concert, hybrid actors screen their action in vagueness and ambiguity, complicating attribution and response. The use of different intermediaries - or proxy actors – supports the achievement of these goals. Hybrid action is cost-effective as it turns the vulnerabilities of the target into a direct strength of the hybrid actor. To reach this essential ambiguity, hybrid actors blur the usual borderlines of international politics and operate in the interstices between external and

internal, legal and illegal and peace and war (interestingly enough, reinterpreting Sun Tzu). This makes hybrid action more difficult to prevent or respond to.

From NATO's point of view the challenges of hybrid action are manifold. Due to the specific character of hybrid threats it is very difficult to create a coherent policy to prevent or respond to them. Concerning the scope and gravity of threat they pose to the target states - including NATO's ability to carry out its core functions – a solid policy to counter them, however, is essential. Here NATO's possibilities to deter hybrid threats form the starting point.

If the tools of deterrence are divided into those of punishment and denial, NATO's challenges can be considered to differ depending on the task in question. The most powerful instrument for punishment is NATO's collective defence with its fifth article of the Washington Treaty as a major deterrent. Hybrid actors scale their operations to stay under the threshold of Article 5 to avoid a collective response from NATO. Inability to respond collectively to hybrid threats remaining below this threshold – or a clear lack of a joint understanding of the place of the threshold *vis-á-vis* hybrid threats – create a serious vulnerability for NATO and its allies. NATO should thus try to safeguard a sufficient internal awareness and consensus about how to respond collectively to hybrid threats taking place under the Article 5 threshold in order to prevent the adversaries from taking advantage of this vulnerability. This requires careful coordination among the allies and close cooperation with the EU as the capabilities to address many forms of hybrid threats taking place in these frameworks. This requires also a good preparedness for a joint attribution of hybrid action that increases the effectiveness of making the threats visible.

Enhancing resilience forms the other part of effective deterrence and here the broad involvement of various branches of government as well as the private sector is the key. NATO must first of all ensure the resilience of its own political and military machinery and take the lead in mapping the vulnerabilities that might constrain its action in a hybrid threat situation. This work has already been launched by strengthening NATO's role in support of its allies for instance in critical infrastructure protection, cyber defence or situational awareness and intelligence sharing. Joint exercises play an important role in testing common decision-making capacity and an enlarged engagement of governmental and private actors has gradually begun.

In this context consolidating NATO's legal resilience is another important goal as an

incoherent legislative framework might seriously hamper collective action against hybrid threats. The ambitious goal of NATO's non-military capacity-building against hybrid threats must be to abolish both political and legal hurdles from an efficient common action and also in this way signal its cohesion in facing the new threats.

Teija Tiilikainen

Director, European Centre of Excellence for Countering Hybrid Threats, Helsinki

She is the Director of the European Centre of Excellence for Countering Hybrid Threats. She was the Director of the Finnish Institute of International Affairs and has also served as Secretary of State at the Ministry for Foreign Affairs of Finland. She is part-time professor at the European University Institute (Florence) and vice-chair of the executive board of the University of Helsinki.

INFOSPHERE: THE NEED TO REVERSE A LOSING TRAJECTORY

Jakub Kalenský

Source: Shutterstock

The West is currently losing the information confrontation with its adversaries. The information aggressors are adapting to the new challenges in the infosphere better than democracies. They are quicker, more aggressive, and more determined to achieve their goals than we in the West are. On the current trajectory, the problems the West faces from the disinformers will be increasing rather than the opposite.

The main reason for this development is the weak reaction of the West to this new type of aggression. There has been no systematic pushback from the democratic states to stop the information aggressors and punish them for their malicious activity — most of the energy of our policy makers is devoted to pressure on social media companies, and to "vaccinating" the targeted audiences via raising awareness. But Russia, China, and others do not face any undesired consequences for their activities in the infosphere, meaning they have no reason to stop.

While the social media platforms are surely an important battlefield, they are not the adversaries; they are an abused channel (by far not the only one and in some audiences, not even the most important one). Similarly, focussing only on the victims of the information aggression and saying that media literacy and supporting fact-checkers solves the problem, is inadequate. We cannot just tell the victims of an aggressor they should be better prepared (that is rather similar to blame a rape victim) and let the aggressor have a free ride. We have to stop the aggressor, but we are not doing that.

That means that the information aggressors only have to adapt to the new, constantly changing environment. What they are doing rather effectively: conspiracy videos deleted from Facebook get uploaded elsewhere and promoted on Facebook again; Russia is getting increasingly skilful in blurring the source of disinformation, and learns how to bypass Facebook's defences; the Kremlin is testing new disinformation tactics in Africa, including the "franchising" of its disinformation campaign, making it yet harder to detect.

Not only are the information aggressors getting more skilful and more experienced, they are also growing in numbers and expanding the area of their activities. Half a year ago, researchers were pointing out that China is applying the Russian infowar playbook in its neighbourhood, in Hong Kong and Taiwan. During the recent COVID-19 crisis, we could see that the Chinese information aggression was increasingly targeting many countries in the West. We see similar measures being applied by Iran and Saudi Arabia, or even by commercial actors offering disinformation for hire, e.g. in China or in Tunisia.

Even an EU member state ran an anti-EU campaign that repeated many speaking points of the pro-Kremlin disinformation campaign of the last years. The PM of the same country was also spreading COVID-related conspiracies that the European Commission itself debunked as disinformation.

Just like any new crime that the authorities do not yet prosecute, also the scale of the problem of the information aggression keeps growing – and will continue to do so until we in the West finally decide to not only demand solutions from the victims targeted by disinformation and from the abused channels, but also try to do something to stop the information aggressors and punish them for their malicious activity.

The Western democracies should face the unpleasant fact that the problem with disinformation campaigns by adversarial actors is increasing rather than decreasing, and

that the reaction so far had been inadequate. Apart from raising the awareness and repairing our own weaknesses, we also have to finally try and stop the information aggressors. We have the tools for that: there is a set of best practices and recommendations to follow; all we need is the political will – and the same determination that our adversaries have.

Jakub Kalenský

Senior Fellow, Digital Forensic Research Lab, Atlantic Council, Washington, D.C.

Jakub Kalenský is Senior Fellow with the Atlantic Council's Digital Forensic Research Lab. In 2015-18, he served in the EU's East StratCom.

ARE AUTONOMOUS WEAPONS ALSO INTELLIGENT?

Antonio Missiroli

Source: businesswire.com

The current debate on autonomous weapon systems involves different policy communities - typically focussed on capability development, deterrence and defence, disarmament and arms control, international law and military ethics – and spans from the possible applications of artificial intelligence (AI) in warfare to widespread concerns about 'killer robots.

The concept of AI dates back to the early 1950s, but technological progress was very slow until the past decade; now it is in full swing. In the domain of public health and diagnostics (e.g. cancer research), these technological developments are already proving their worth, and their benefits are uncontested. In the field of security and defence, however, the jury is still out: the prospect of fully autonomous weapon systems, in particular, has raised a number of ethical, legal and operational concerns.

'Autonomy' in weapon systems is a **contested** concept at international level, subject as it is to different interpretations of its levels of acceptability. The resulting debate triggered for

instance the establishment at the United Nations, in 2016, of a group of governmental experts (GGE) on Lethal Autonomous Weapon Systems (LAWS) , that until now was unable to reach agreed conclusions. This is in part due to the current strategic landscape and the 'geopolitics' of technology, whereby some states developing these systems have no interest in putting regulations in place while they believe they can still gain a comparative advantage over others.

Yet it is also due to the fact that 'autonomy' is also a **relative** concept. Few analysts would contest that, in a compromised tactical environment, some level of autonomy is crucial for an unmanned platform to remain a viable operational tool. Moreover, *automatic* weapon systems have long existed (e.g. landmines), and *automated* systems are already being used for civilian and force protection purposes, from Israel's 'Iron Dome' missile defence system to sensor-based artillery on warships. In practice, with very few exceptions, current weapon systems should be considered, at best, *semi-autonomous* – and they tend to be extremely expensive and thus hardly expendable.

In fact, there are still technological as well as operational limits to the possible use of LAWS: while engaging targets is getting ever easier, the risk of miscalculation, escalatory effects and lack of accountability (all potential challenges to established international norms and laws of armed conflict) seem to favour maintaining meaningful human control ('man in the loop'). Yet the temptation to exploit a temporary technological advantage through a first strike also remains; not all relevant and capable actors may play by the same (ethical and legal) rules.

In the past, international efforts to control the proliferation, production, development or deployment of new military technologies (from CBRN to landmines, from blinding lasers to missile defence systems) were all, to various degrees, driven by four distinct but potentially overlapping rationales: ethics, legality, stability and safety. The possible military use of AI, especially when related to 'standoff' weapons, has raised concerns on all four grounds. In the past, again, apparently inevitable arms races in those new fields have been slowed or even halted through some institutionalization of norms, mostly achieved after those technologies had reached a certain degree of maturity - and often advocated, inspired and even drafted by communities of relevant experts (from government and/or academia).

The risk of an arms race in these new technologies undeniably exists. Yet so does the hope

that such technologies may still be channelled into less disruptive applications and end up in the same category as poison gas or anti-satellite weapons - in which the most powerful states will abstain from attacking each other (at least militarily) while weaker states or non-state actors may still attack, but to little effect.

* *Dr Missiroli writes here in a personal capacity.*

Antonio Missiroli

Former Assistant Secretary General, Emerging Security Challenges Division, NATO, Brussels

Dr Antonio Missiroli is the former Assistant Secretary General for Emerging Security Challenges. He was the Director of the European Union Institute for Security Studies in Paris, Adviser at the Bureau of European Policy Advisers of the European Commission and Director of Studies at the European Policy Centre in Brussels. Currently, he is Non-Resident Research Fellow in the Nato Defense College Research Division.

Evolving issues

ENERGY SECURITY

Massimo Nicolazzi

Source: tnnltd.uk

Once upon a time energy security was achieved through military control; in fact, the British army conveniently forgot that World War I was over and kept marching until it reached the (presumed) oil reserves in Kirkuk.

Successively it was mostly American security, with the US producing in the 30s even more than 70% of global production, World War II being fought effectively between the Haves (petroleum) and the Have Nots (the Axis), with the Oil Majors granting the integration of Middle East production into the American system.

The year 1973 marked the first big shock. Producing countries had become independent; while the USA and the West truly dependent on their oil. Hence a security paradigm i.e. the security of being supplied and at affordable prices. In other words, and with a bit of historic irony, a sort of bill of rights of the importers.

However, that paradigm may become quickly obsolete. The present market has on the one hand increased importers' freedom and on the other resources' rent has diminished

freedom from the producers; thus the age of supply abundance has further penalised the supply side.

Market first. Oil transportation being an immaterial cost, the market gets liquid. To quote the oil economist Morris Adelman, "*The oil market, like the ocean, is a great pool*". Replaceability of the producer, unless refining constraints are taken into account, is de facto granted and trading at open prices rules out price any fixing by the producers. The posted price system has gone; market price defines per se "affordability". Furthermore, the decrease of energy intensity in productive process makes the West further resilient to potential price spikes.

Resources rent comes second. Since exporters are more and more dependent on oil price for their budget (therefore for their welfare and their ability to prevent or at least contain social unrest), the consequence is that they have lost the freedom to withhold sales. So, the old West's nightmare of embargoes is just a (false) memory. The last attempt by Venezuela ended up almost in mockery, just confirming that embargoing today is an importer and not a producer game. Iran is an excellent case in the matter.

Last but not least, abundance. The more recurrent problem with oil is that there is too much of it. The pandemic may hopefully be temporary; but gas prices had collapsed well before and the oversupply of oil dates back to 2014. Abundance has meant a demand driven market and immunity from current outages (we cancelled Libya and Iran from the market, and the price did not bulge).
Market and abundance have thus somehow depoliticised the security issue. The favourite argument within some Atlantic communities was traditionally to cry wolf due to the security threat involved by the EU "dependency" from Russian gas. Now we are discovering that the dependence was (also) a price signal and we kept buying more just because it was cheaper.

As soon as Asian markets crashed, LNG started sailing to Europe; and in 2020 we have had months when EU has imported significantly higher volumes of LNG than Russian pipeline gas. If one considers that, due to current price mechanisms, Russia pipeline gas is a price taker and not a price maker, the wolf may look much more manageable.

The emphasis shifts then from security of supply to security of infrastructure, including (as the future will be more and more electric) security of the grid. The ability to secure

energy flows irrespective of potential outages and the prevention of outages via technologic or traditional security.

Prevention may however not be ever successful. Plan B is that if you cannot prevent outages, be they technical or political, you should then prevent them from being disruptive. The mantra since 1973 has been "diversification of supply" i.e. more suppliers = less risk. The implied focus was on the potential for political outages, while technical problems were left to the individual nation States to cope with.

However, since then national grids and networks on the European side of the Atlantic were gradually integrated (and integration with its inbuilt flexibility is an important security factor) and during the same period there were no major disruptions due to "political" outages. For instance, in Italy the biggest disruption ever has been a day-long electric black out in September 2003; not a terrorist act, just a couple of Swiss trees falling over the electric cables connected to Italy.

Some broader standard could then be introduced, like shifting from diversification of supply to the provision of a quantum of redundancy. To tackle emergencies the first remedy is having reserves in stock (gas storage, batteries, etc.) and/or having built in the system a substantial transportation and distribution overcapacity and/or an increase of the electric grid resilience. The quantum of security becomes almost an inverse function of the load factor of the system.

Redundancy is not for free and therefor security becomes mainly a cost issue. It is basically the substitute for an insurance policy and since a total insurance will never be feasible, someone has to decide the quantum of insurance to be factored in the system. Whoever it may be, a preliminary talk with the taxpayer is advisable; after all we are dealing with public money.

Massimo Nicolazzi

President, Centrex Italia SpA, Milan

With almost 35 years of experience in the hydrocarbon sector, Massimo Nicolazzi worked for Eni and Lukoil before being appointed CEO of Centrex Europe. Today he is Chairman of Centrex Italia SpA and Senior Advisor of ISPI's Energy Security Program. He has written several publications and he is member of the Italian Geopolitical Magazine "Limes".

SPACE IS NOT A HIGH GROUND

Bleddyn E. Bowen

Source: Shutterstock

Headlines have again been made by a state testing a direct-ascent anti-satellite (DA-ASAT) weapon system. Russia's flight test of its Nudol missile technology (which some claim is more for missile defence) falls into a wider and longer-term pattern of DA-ASAT weapons testing and development which has seen the United States, China, and India conduct similar flights over the last 15 years.

Some responses are entirely too predictable and turgid where blame for 'militarising space' or 'destabilising' the international environment is cast around with no consideration for the actions of other states in tolerating or even conducting such activities. Indeed, such commentary was not missing when NATO declared space an operational domain in 2019.

Whilst such criticism tends to ignore the fact that space has been used for military purposes since the dawn of the Space Age and that several space powers have piecemeal anti-satellite weapon projects, declaring space the 'ultimate high ground' is another favourite among military space writers and many space practitioners.

Capturing and holding a high ground usually means that you gain some advantages over

your adversary by possessing good defensive positions or places to launch efficient offensives from. Space weapons (Earth or space-based) are seen as methods of seizing or denying the control of this 'ultimate high ground'.

Space systems in orbit undoubtedly provide important services and military advantages to modernised terrestrial military forces. Some would struggle to do without these services today. But the 'ultimate high ground' moniker is used as way to justify or imply that defending assets in space is needed at all costs, where if secured or a preferred technological system is invented, victory is sure to follow.

In practice it means merely somewhere where there is an advantage to be gained. It is a banal and generic term that can mean anything that provides an advantage. Space is important and very useful, in some specific campaigns even essential, but it exists in a far larger strategic context.

High grounds need a lot of other things to go right to be significant: logistics, morale, political support, competent command, incompetent enemies, timing, and no small amount of luck. Successive American, Israeli, British, and Russian military surprises in the 21st century should be plain enough to demonstrate that the principle of assured space control fails to prevent political upset or strategic failure.

Without its own space-based assets, NATO needs to think about how it can better coordinate the military space spending and capabilities of its member states, and the idea of the 'high ground' does nothing to help frame such debates and discussions. Where can allies make the biggest difference and contributions to the existing space capabilities of its larger member states? Where can duplication be avoided? NATO's primary concerns should be on building a more resilient and responsive space infrastructure and avoiding the intellectual dead ends of thinking about space as a high ground because this ground is only relevant in high-intensity warfare and will be the purview only of the largest and best-funded military powers.

The advantages of controlling space must be consciously exploited in the other environments on Earth. Space power's effects from orbit can be blunted as well as exploited in Earth's other environments. In short, controlling space by itself does not give you a decisive control of Earth. Dominating space and controlling 'the ultimate high ground' will not give you victory by itself, but it is certainly useful to have.

**This is a highly condensed and revised version of a column originally written for Spacewatch. Global, which is available here: https://spacewatch.global/2020/04/spacewatch-column-april/*

Bleddyn E. Bowen

Lecturer in International Relations, University of Leicester, Leicester

Dr Bleddyn E. Bowen is a Lecturer in International Relations at the University of Leicester. He is an expert in space warfare and space policy, and author of "War in Space: Strategy, Spacepower, Geopolitics" (Edinburgh University Press). He has published in several academic journals and engages frequently with policy and military space communities.

NON-STATE ACTORS EMPOWERMENT IN THE MIDDLE EAST

Rami G. Khouri

Source: middleeasteye.net

Most of the Middle East's serious problems – wars, terrorism, foreign militarism, politicized sectarianism, refugee flows, mass poverty and vulnerability – reflect the consequences of the two great overarching trends in the past century of the modern Arab state system.

In the first half of the century, broadly from 1920 to 1970, the Arab region completed impressive state-building processes that steadily improved citizens' quality of life.

In the century's second half, from 1970-2020, about half the Arab states have seen their state-building momentum stall or even reverse. Economic and social development slowed after 1990 when most non-oil-financed governments could no longer improve or even maintain the quality of life of large swaths of their populations.

The UN today says that at least 70% of all Arabs are poor or vulnerable, and that figure is rising daily due to the economic impact of the oil price drop and the Covid-19 pandemic.

Two important dynamics emerged that led to the rise of non-state actors (NSAs):

1. some states started to fragment as local authorities affirmed their authority over a weakened central government (Sudan, Iraq, Lebanon, Yemen);
2. in every non-oil-rich country, non-state actors assumed a bigger direct role in providing citizens services they had obtained from the state during the previous three generations (security, identity, political voice, material assistance, and basic services).

Some NSAs became so powerful that they paralleled the central government in some places (Muslim Brotherhood, Hezbollah, Kurdish groups) or even replaced it in others (Hamas, Islamic State, Kurdistan, Insarullah-Houthis, South Sudan rebels). Powerful armed NSAs, like Hezbollah, Hamas, and Insarullah-Houthis, took over the national security role of the state and also provided basic services.

Other armed groups like Popular Mobilization Forces (PMF) militias in Iraq, complemented the state's security operations against threats like Islamic State, and PMFs in Syria, Yemen, or Libya have been created, funded, trained, and armed by foreign powers (regional ones like Iran, Turkey, the UAE, Saudi Arabia and Israel, or foreign powers like the USA).

Hundreds of NSAs across the region are unarmed civilian groups that are anchored in the two most powerful forces that existed before the modern state arrived: religious and tribal identities. The modern state usually could not control or co-opt these powerful forces, and mostly coexists with them. When central governments in the 1990s started contracting and ignoring large population segments, the tribal and religious NSAs stepped in smoothly. Some of them in Syria, Iraq, Libya, and Yemen also became politicized and frequently sought a share of government power.

The first big sign of Arab citizens discontent that translated into stronger NSAs was the rapid expansion of the Muslim Brotherhood and other such Islamists in the mid-1970s. This was due to multiple factors, including: the humiliation of the June 1967 Arab defeat by Israel; the failure of socialism, Arab nationalism, Ba'athism, and capitalism to meet citizen needs equitably; government corruption due to incompetent rule by family- and military-based regimes; and, the stresses of inflation and high living costs that sent several hundred million Arabs into poverty.

As citizens steadily lost trust in the central state's credibility, and its legitimacy in some

cases, after the 1980s, they increasingly turned to NSAs for their essential personal, communal, and political needs. NSAs like the Muslim Brotherhood grew stronger and often shared power, due to several reasons: they focus squarely on citizens' basic needs, they are anchored in the communities they serve and speak in social justice terms that resonate with citizens, they are mostly uncorrupted by massive money flows, and they emphasize equitable socio-economic development at home and confronting aggression from abroad.

Rami G. Khouri

Senior Fellow, American University of Beirut, and Journalist-in-residence, Beirut

Rami G. Khouri has reported in the Middle East for 50 years. He is journalist-in-residence and a senior public policy fellow at the American University of Beirut, and a non-resident senior fellow at the Harvard Kennedy School.

WEAPONS OF MASS DESTRUCTION

Eric R. Terzuolo

Source: www.vitalykuzmin.net

Weapons of mass destruction have been on NATO's agenda since the early days of the Alliance and will remain there. The NATO nuclear deterrent, a careful collaboration between the United States and the European allies, seems destined to remain an important transatlantic link. NATO remains an indispensable forum for consultation and, to some degree, joint decision making on arms control and countering WMD proliferation. The Alliance also has proved itself a **valuable tool** for building the capacity of the Allies and partner countries to deal with WMD threats and for sharing information on such threats.

No surprise that **NATO's 2010 Strategic Concept** committed the Alliance to continue active engagement on arms control, non-proliferation and disarmament. On the 5th of March of this year, for example, the North Atlantic Council (NAC) issued a **statement** celebrating the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) on the 50th anniversary of its entry into force.

But such declarations are ringing empty these days. Alliance leaders should accept that we

are entering, or perhaps already have entered, a *post-arms control* and *post-non-proliferation* era. A June 2020 **special report** in *The Economist* was eloquently titled: "The clock is ticking for nuclear arms control." But even that was perhaps too optimistic; it can be hard to accept the deterioration of the post-war international security order, but we clearly are moving back to a more Hobbesian international reality. Not yet the war of all against all, but some key powers are embracing a more conflictual world view, with self-help as the watchword.

There is plenty of blame to go around. As NATO rightly agreed, **Russia had violated** the INF Treaty with the deployment of SSC-8 cruise missiles, but it was the United States that actually withdrew, putting an end to the treaty, and its inherent rules of international conduct. It is difficult to be optimistic about a renewal of the **New START Treaty** before it expires in early February the next year. The Trump Administration's insistence on bringing in China, an entirely different sort of nuclear power, is a likely deal breaker. Chronic Russian sabre rattling does not help, neither is the USA explicitly keeping the door open to **renewed nuclear testing**.

The international non-proliferation regime, in turn, has proved itself incapable of blocking North Korea from joining the club of de facto nuclear powers. And the often-praised, now in practice defunct nuclear deal with Iran, at its best, entailed great expenditure of political capital to achieve a limited and temporary objective.

Trying to turn back the clock to a more norm- and regime-based era could be a waste of time and political energy. Perhaps NATO's focus should be on individual countries and promoting responsible conduct. US ability to exercise leadership in the Alliance will be key. Everyone at NATO HQ has been walking on eggshells, but there are prospects for positive near-term change in Washington. Former Vice President Biden has a strong record of responsible approaches to WMD and other security challenges. US allies should prepare to seize the moment, and signal clearly their expectations for genuine, proactive intra-Alliance collaboration.

Putin and Xi, though, are not going anywhere. Regime transformation is improbable in Iran and North Korea. Could NATO, however, become *the* place for deciding how to use the resources of the Alliance countries to promote change in the policies of such countries of concern? The Alliance's primary added value arguably has always been as the key forum for transatlantic deliberation and decision making.

At the same time, NATO's relevance in nuclear deterrence and in promoting the ability of Allied and partner countries to deal with nuclear, radiological, chemical, and biological threats will remain. Perhaps even accentuated as control regimes deteriorate. NATO, in sum, is not an arms control or non-proliferation organization as such, but does have an important role to play.

Eric R. Terzuolo

Professorial Lecturer, School of International Service, American University, Washington, D.C.

Eric R. Terzuolo is a teacher, scholar and practitioner of international relations, with particular expertise in European politics, NATO affairs, arms control, and non-proliferation. From 2010 until recently, he was contract to the US Foreign Service Institute, the Department of State's training unit, with responsibility for West European area studies.

@NATO Foundation

@NATOFoundation

NATO College Foundation

@natofoundation

info@natofoundation.org