SAFER TOMORROW: SECURITY STARTS WITH YOU(TH)

Policy Brief
September 2022

ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

NATO OTAN

This Policy Brief is promoted by the NATO Public Diplomacy Division

An initiative by the Center for the Governance of Change at IE University in collaboration with the NATO Public Diplomacy Division, launched on June 28th, 2022, during a morning of panel discussions dedicated to understanding the interconnection between emerging technologies and international security.

ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

NATO OTAN

OPENING REMARKS

Irene Blázquez

Director, Center for the Governance of Change

On June the 28th, the Center for the Governance of Change (CGC) at IE University had the great pleasure and honor to convene an extraordinary group of authorities, colleagues and friends at the launch event of our Safer Tomorrow Initiative: Security Starts with YOU(TH), an initiative promoted by NATO's Public Diplomacy Division and supported by the CESEDEN (Spain´s Centre for Advanced National Defense Studies) and the National Security Department at the Cabinet of the Spanish Prime Minister.

Hours before the Madrid Summit, a Summit dominated by Russia's aggression against Ukraine, where NATO Leaders were going to adopt a new Strategic Concept, the fourth public post-Cold War Strategic Concept, the core assumptions that shaped NATO's previous Strategic Concepts were no longer valid: war is back to Europe, great power competition is rising and multilateralism and the rules-based international order are in decline and jeopardized.

At the CGC, an applied-research, educational institution that studies the impact and implications of the current technological revolution on politics, prosperity and power (meaning security and defense), we felt that it was extremely timely, before the new Strategic Concept was adopted, to gather top-level academics, thinkers and practitioners, relevant and diverse voices, to reflect on defense, crisis management and cooperative security.

As regards, the longer-term and systemic threats, technology has not only transformed the nature of power but also its balance and distribution across states and organizations and beyond states. The Spanish Foreign Action Strategy 2021-2024, which was released under the leadership of Minister González Laya, recognizes that technology and innovation are shaping a new global order.

The future security of the Alliance will depend on its capacity to implement, on the one hand, disruptive technologies such as Data, Artificial Intelligence, Autonomy, Space Technologies, Hypersonic Weapon Systems and, on the other hand, emerging technologies including Quantum, Biotechnology and New Materials.

We had the pleasure of counting that morning with an extraordinary first panel that revolved around the ability of the Alliance to preserve its technological edge in a way aligned with the NATO 2030 Initiative, to foster cooperation vis-à-vis China, and to reinforce the Alliance's resilience. A special space was devoted to climate change as a systemic shift and Russia's nuclear threats in the war against Ukraine was on the table for debate.

As regards immediate threats, the new Strategic Concept was set to look at how to strengthen defense and deterrence along NATO's eastern flank. NATO faces a liquid security environment with critical challenges in the six domains of operations coming from state and non-state actors: hybrid warfare, cyber threats, and information operations altogether are the new normal. The example of Ukraine is telling.

Our second panel discussed on how hybrid warfare has evolved in the aggression and what role cyber and disinformation play in the changing nature of international conflict. We could extend a warm welcome back to his home to Oscar Jonsson, former Academic Director of the CGC, who discussed these topics in this outstanding panel.

To frame this huge debate on how technological disruption and other systemic challenges alongside with the immediate threat posed by Russia's aggression against Ukraine will impact on NATO's core tasks and priorities, we were honored to have General Torcal, who offered some opening remarks, and Former Minister and Dean González Laya as our keynote speaker, who discussed the new security landscape and the changing global order.

We knew we were about to witness a historic and transformative NATO Summit. A milestone, as it was concluded in the Madrid Declaration adopted the 29th June. The New Strategic Concept has moved significantly forward on the consideration of technology as a key element of the security and defense landscape granting certain gravitational force to emerging and disruptive technologies in its roadmap.

This CGC's initiative aims at building a likeminded community, which goes above and beyond the kickoff encounter, to discuss and produce applied research on security, defense and technology in future and upcoming occasions involving and engaging youth. What is at stake is the totality of the international liberal and democratic order.

We wish to express our heartfelt appreciation for making possible what it turned out to be a very successful event of enlightenment possible to the Alliance and particularly to Paula Redondo for her witty understanding of the project and her insightful participation in our second panel. A special thank you to the CESEDEN, the National Security Department, Former Minister and Dean González Laya, General Torcal as well as all our incredible speakers, the nice and esteemed audience and our colleagues and friends at IE University for their support.

Last but not least, I would like to extend a particularly warm and affectionate thank to Paula Martínez López, Research Program Coordinator at the CGC, and Lourdes Zurdo, Coordinator at the CGC. Paula deserves a very special recognition for enthusiastically, impeccably and constantly pushing forward our Safer Tomorrow Initiative. Lourdes Zurdo Varela was also instrumental in the success of the launching of the initiative as a discreet but fundamental member of the CGC.

We look forward to continuing our conversation in the next meeting of our program.

Foreword by

General Luis Torcal

Director, Department of Defense Culture and Diplomacy, CESEDEN *(Centro Superior de Estudios de Defensa)*

It was a real privilege to have the opportunity to deliver the opening remarks at the conference “Safer Tomorrow” held by the Center for the Governance of Change at IE University on the 28th of June. I believe that the timing of its celebration could not have been more opportune, just on the eve of the NATO summit in Madrid.

On that occasion, I tried to emphasize two main ideas that I consider to be of the greatest importance.

The first one is that we live in extremely volatile times. Events are happening right now that were unthinkable until recently. Simultaneously, these events demonstrate the persistence of lines of confrontation and crisis that have repeatedly manifested themselves throughout history, and in which geography and cultural differences continue to play a very relevant role.

In less than a year, and with the world facing the COVID pandemic, we have experienced: the return to power by the Taliban in Afghanistan; the revitalization of the defense pillar of the European Union with the approval of the "Strategic Compass"; Russia's attack on Ukraine; and the approval of a new NATO Strategic Concept, breathing new life into an organization thought less than a year ago to be brain-dead.

The second idea I defend is that technology has always influenced the way combat is executed. This is obvious when looking at the changes in combat modes throughout history. But the corollary of this idea is that technology, no matter how influential it may be, does not determine the outcome of a conflict. With each new technological advance, there has been a reaction that has made it possible to confront and rebalance the advantage. Ultimately, as the images from the Ukraine war show, victory is only achieved when the enemy forces are driven out and the ground is occupied. As we Spaniards demonstrated in the confrontation with Napoleon, the Vietnamese in the war against the Americans, the Afghans in their opposition to the foreign presence in their country, and the Ukrainians in their defense against the Russian attack, the results of the combat depend not only on technology but also on the behavior of human beings motivated by moral values.

What differentiates the current era from past times is that technological development has accelerated and affects all domains of the conflict. The classics of land, sea and air have been joined by cyberspace, outer space and the cognitive domain. In addition, our time is dominated by global knowledge and the almost instantaneous diffusion of what happens in any part of the world. Therefore, the model of confrontation that we are facing implies the availability of means and the preparation to act in a lethal and precise manner in these multiple areas. Some nations are less than averse to taking casualties in combat. That is not the case in Western nations. But military equipment and training is expensive and will always come at the expense of other needs to be covered.

War is certainly expensive. But we may remember that defeat costs more.

KEY TAKEAWAYS

PANEL 1

Emerging technologies and international security: Lessons for the Madrid Strategic Concept

Emerging and disruptive technologies such as artificial intelligence (AI), autonomous weapons systems or quantum technologies are transforming the international security landscape and impacting the way NATO countries operate. The 2010 Strategic Concept failed to consider these critical areas, however, NATO has now put its focus on nine innovation areas, including: AI, data, autonomy, quantum technologies, biotech and human enhancements, hypersonic tech, space, novel materials and energy. As conflict becomes increasingly hybrid, the development of innovation funds, accelerators and transatlantic cooperation on these critical technologies to advance interoperability and address these new threats becomes paramount.

These were the topics covered by the first panel, moderated by **Carlos Luca de Tena**, Executive Director, Center for the Governance of Change.

PANELISTS

Antonio Notario

Head of the Political-Strategic Planning Unit, National Security Department, Office of the Spanish Prime Minister

Katarina Kertysova

Policy Fellow, European Leadership Network (ELN)

Lydia Wachs

Research Associate, Stiftung Wissenschaft und Politik (SWP)

Margarita Konaev

Research Fellow, Center for Security and Emerging Technology (CSET), Georgetown University

Bernardo Navazo

Associate Professor of International Security Politics and International Relations and Defense Analyst, Universidad Carlos III

ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

NATO OTAN

How is technology transforming the global security scenario?

Antonio Notario

First, the international system born after the Second World War was designed for the exchange of money and physical goods, not for data and software. That inadequacy is visible in a fragmented landscape, with two spheres of technological influence replicating the political map; on the one side, the Partnership for Global Infrastructure and Investment, on the other side, the One Belt, One Road Initiative.

Second, in terms of geopolitics, technology is the new metrics for national power. That leads to a global race for tech dominance. Technology broadens the spectrum of threats to national security, accelerates the rhythm of change and injects technical sophistication.

Third, from the point of view of the digital economy and markets, one of the key drivers of the global context is the complex interdependence. This is an euphemistic way of referring to the technological asymmetries. New strategic dependencies appear as a consequence of digital progress. Today, semiconductors, raw materials, software and biotechnology are used as elements of diplomatic leverage.

To sum up, these three dimensions ¾ spheres of technological influence, national security and asymmetric connections ¾ are strongly interrelated, where technology is seen as the common factor of strategic advantage.

Katarina Kertysova

Allied militaries rely heavily on fossil fuels. From an operational point of view, fuel supply convoys have often come under attack on the battlefield. With fuel supply infrastructure being attacked in Ukraine, the war has once again shown that fuel dependency in the military is a big vulnerability. During his speech at the NATO Public Forum, Secretary General Jens Stoltenberg stressed that "the most efficient armed forces will be those that do not rely on fossil fuels." Stoltenberg further noted that as we shift away from fossil fuels, we must ensure that we do not swap one dependency for another – namely dependence on countries like China for raw materials that are essential for the clean energy transition.

Technological innovation plays an important role in this regard. As I noted during the June 28 kick-off event, many of the technological solutions that can help our militaries lower their fuel use already exist. Deliveries by drones or 3D printing of weapon components and ammunition at the point of use can significantly reduce fuel use on the battlefield. Sustainable aviation fuels are increasingly being used too. Many Allies are already electrifying their white fleets. Improving energy efficiency of buildings and bases constitutes another low-hanging fruit. When it comes to emerging technologies, as AI and computing power develop, we will be increasingly able to train and exercise digitally. With 5G and space-based observing systems, our militaries will be able to plan their operations in a more efficient way in the future. Additional investment in R&D programs will be needed to reduce the energy consumption of heavy-weapons systems. We also need more resource-efficient and, eventually, climate-neutral production processes. Now that Allies invest more in defense, we need to make sure that these additional budgets are also used for R&D initiatives oriented towards sustainable solutions.

How is technology transforming the global security scenario?

Lydia Wachs

Technology is changing the global security context. But this is not a new development – technological advances and innovation have also in the past affected the security landscape and will continue to do so. In addition, technology is not deterministic – it is not technology per se that potentially has strategic effects but the way we use it and the way in which it is exploited in the military domain. Therefore, it is extremely difficult, if not impossible, to assess the net effect of emerging and disruptive technologies (EDTs) on security and stability. This is compounded by the fact that, for example, AI is a general-purpose technology that can be applied in many different ways and in various contexts, both in the civilian and military domain. Clearly, EDTs like AI and autonomy entail opportunities – for example faster information processing that allows for better decision-making. But there are also risks raised by EDTs, like AI. In particular, enduring technical shortcomings with AI, risks stemming from human-machine interaction as well as an accelerated tempo of warfare that undermines effective human control could present challenges to stability by exacerbating escalation dynamics.

Margarita Konaev

There is no single way that technology is affecting global security, rather, we must prepare to think flexibly about potential contingencies and become more comfortable with uncertainty and even contradiction.

For instance, experts disagree about the trajectory of AI development - some expecting revolutionary breakthroughs while others anticipating another "AI winter" where progress is halted.

Another example are opposing views on who will benefit from progress in AI – will it turn weather, more tech advanced countries even more powerful, economically, militarily, etc., or will it serve as an equalizer, democratizing access to information, and allowing for the proliferation of advanced tech to non-state actors (as was the case with drone tech)? This is why we must become comfortable with ambivalence in our assessments, and be prepared for numerous, often contradictory eventualities.

Bernardo Navazo

I would turn the question around and argue that it is the current global security scenario today, namely the return of great power competition, that is accelerating both scientific advancements and technological applications mainly on the military end. As the classics put it, the lust for power is an immense incentive to employ all the levers available, science and technology being one of them. Obtaining a winning edge, as small as it might be, on your geopolitical struggle by capitalizing on science and technology leads governments to increase funding on both applied and pure science. Thus periods of intense geopolitical competition galvanize scientific and technology production. Science and tech, as any other area in which human beings are immersed, are highly political.

Today's scientific races (cyber, hypersonic weapons, AI) only differ from those of other periods (i.e., planes, tanks and chemical weapons in the WWI; radar and nuclear weapons in WWII; space race during the Cold War; the fight between carbon-propelled, iron-hulled warrying boats versus new oil-propelled, steel-hulled ones in the turn of the XX century) in name and the scientific content itself, but not at all in its political dimension. Today's tech competitions are tantamount to those of yesterday.

What technological challenges caused by emerging and disruptive technologies (EDTs) should NATO envision?

Antonio Notario

Lydia Wachs

The consequences of emerging and disruptive technologies have been included in the analysis of the current security environment in the NATO Strategic Concept 2022.

It is interesting to note possible actions which could led to the invocation of Article V of the North Atlantic Treaty. Whilst in 2010, the only reason included was an armed attack, the new Strategic Concept expands on this and mentions three possible actions that could reach the level of such an armed attack:

- A single or cumulative set of malicious cyber activities.
- A hostile operation to, from, or within space.
- A hybrid operation against Allies.

Second, in relation to Crisis Prevention and Management, big data and deep learning are two emerging technologies with huge potential to improve risk assessment and strategic foresight. Also in this field, the space programs are having a huge impact in situational awareness though intelligence, surveillance and reconnaissance tasks.

Third, dealing with cooperative security, I see a clear evolution in training from the current war gaming to virtual reality solutions, not to mention the future employment of the metaverse.

The Strategic Concept as a broad strategy document can only include a recognition of the fact that EDTs are changing the security context and hold both opportunities but also risks. This notwithstanding, there are two kinds of challenges NATO has to address in the coming years with regard to EDTs: external and internal challenges.

External challenges concern the use of EDTs by strategic competitors and potential adversaries. For NATO, especially Russia's development and use of EDTs presents a challenge to the security of the Alliance. Russia views the development of EDTs for military purposes as essential and has invested heavily in research and development, while developing a new innovation infrastructure. Furthermore, it is adapting its military concepts to include the use of, for example, AI-enabled capabilities and weapon systems with autonomous functions. At the same time, it rejects an international regulation of weapon autonomy. While Russia is struggling with both structural problems as well as problems due to the heavy Western sanctions, it will likely continue to exploit EDTs for asymmetric benefit.

In terms of internal challenges, NATO allies hold different views on the development and use of EDTs. This is true particularly with regard to the use of AI. While the Alliance adopted six principles for the responsible use of AI in 2021, the operationalization and implementation of these principles will be much harder as allies remain divided on the ethical and legal specifics of the military use of AI and autonomy. In addition, there is also a divide in terms of technological capacity and the willingness to share data. Failing to bridge these technological gaps and different approaches could in the long run undermine interoperability and weaken Alliance cohesion.

What technological challenges caused by emerging and disruptive technologies (EDTs) should NATO envision?

Margarita Konaev

I would argue that it's not necessarily about the technological challenges themselves, but rather about NATO's ability to react or even better, anticipate alternative futures, and as such, invest in force structure, training, and strategic thinking that can handle unexpected developments and adjust accordingly. That said, to be more specific, some of the key challenges NATO must contend with is that unequal progress and adoption of emerging tech like AI could exacerbate the already severe gap in military capabilities between the NATO allies, which may in turn undermine interoperability and the alliance's military effectiveness. The impact of EDT's on the information environment is of course another major challenge facing NATO, with the potential to deepen political fissures and undermine cohesion.

Bernardo Navazo

The acceleration of times has baffled us: technological breakthroughs are observed almost on a daily basis and not only limited to traditional academic or scientific hubs (American universities or the likes of Silicon Valley). Patents, developments, new products or new tech applications go to the market every single day. That is one of the benefits of globalization and the advent of global epistemological communities (one for each tech vertical) thanks to Internet. The negative side is that some of those developments may have either military applications or alter the current balance of power. 5G, cyber, unexpensive-but-highly-effective drones, AI and autonomous weapons are the cases at hand. Keeping track of all these developments in so many areas is a daunting task even if one limits its focus to open sources, open patents, and the like.

Include the secrecy around other technological developments (for example, China's hypersonic programs) and the task expands. Thus monitoring and identifying these breakthroughs is absolutely critical.

How to operationalize this task? The EU-US Trade and Technology Council (TTC) comes to my mind. As the reader surely knows, the TTC is a forum where Washington and Brussels frequently meet to discuss trade issues and exchange information on sensitive technologies. Curiously enough, the trade side of the TTC faces several challenges (for the EU and the US do not look into each other's eyes here). But the technology side is working extremely well: both sides feel the need to institutionalize a Bentham panopticum on any technology that could threaten our economy (i.e., supply chain disruptions on microchips, semiconductors, renewable energy products and the like) or our societies (i.e., biometrics, privacy and data managements, etc.).

Thus is a logical corollary that a military counterpart of the TTC is needed and that a NATO Military Technology Council is a sensible way to go. Such a move would further deepen EU-US relations on issues in which both political communities are aligned: sharing cultural and political values that are to be protected and could be threatened by certain technologies.

Regarding the technological dimension, what synergies should be promoted between the Common Security and Defense Policy (CSDP) of the European Union and the new NATO Strategic Concept?

Antonio Notario

The central framework is the EU-NATO cooperation agreement, signed at the Warsaw Summit and updated one year later, in 2017, with 74 actions.

Moreover, the triangle formed by the European Defense Fund, with 8 million euros; the Coordinated Review of Defense, whose priorities are to develop next generation capabilities; and the Permanent Structured Cooperation, best known as PESCO, have a strong component on innovation, research and emerging technologies. For example, the new surface warship program is focused on electromagnetic weapons, smart damage control systems, multi-domain combat cloud, passive radars and quantum secure communications.

Additionally, it is important to note the new Defense Innovation Fund, established this year under the umbrella of the European Defense Agency. This new initiative, with a budget of 2 billion euros, will stimulate the cooperation between Member States in defense and industrial innovation, in security applications based on AI, for example.

On the NATO side, the new Strategic Concept is not the only document to be approved during the Madrid Summit. The new Defense Innovation Accelerator for the North Atlantic will create a network called "Triple Hellix" between NATO itself, academic institutions and start ups for researching the impact of emerging technologies on security and defense.

Katarina Kertysova

Climate change is a collective action problem. No one is immune from its impacts and no institution alone has all the answers. The newly adopted Strategic Concept recognizes this challenge and calls for enhanced NATO-EU cooperation on issues of common interest, including the impact of climate change on security. When it comes to innovation and green technologies, these are ultimately investment decisions. NATO has limited collective financial means in the civilian budget to do more on climate change. The EU has such funding mechanisms in place, through PESCO, the European Defense Fund (EDF), or various programs of the European Defense Agency (EDA)1.

According to Katarina Kertysova, "given the limited funding that is available, NATO and the EU should align on stimulating green innovation and R&D. The newly launched NATO Innovation Fund and the Defense Innovation Accelerator for the North Atlantic (DIANA), should be complementary with existing EU efforts and avoid duplicative programs. The EDA, which serves as a hub for European defense technology and innovation and is further ahead in this area than NATO, should facilitate closer EU-NATO cooperation as DIANA takes shape."

[1] See Louise van Schaik et al. The World Climate and Security Report 2022: Decarbonized Defense - Need for Clean Military Power in the Age of Climate Change, Center for Climate and Security, an institute of the Council on Strategic Risks, June 2022.

Regarding the technological dimension, what synergies should be promoted between the Common Security and Defense Policy (CSDP) of the European Union and the new NATO Strategic Concept?

Lydia Wachs

What we are currently seeing is a proliferation of agencies and initiatives both by NATO and the EU that are tasked with stimulating innovation in EDTs, including for security and defense. The EU is seeking to foster collaborative innovation through the European Defense Agency and specifically the European Defense Fund (EDF), aimed at supporting cooperation in defense technology and equipment as well as PESCO that is supposed to deepen defense cooperation to deliver the required capabilities. In addition, the EU Strategic Compass established a new Defense Innovation Hub. Within NATO, similar mechanisms and initiatives were set up, inter alia the Defense Innovation Accelerator for the North Atlantic (DIANA) and the Innovation Fund. Beyond these institutional bodies and mechanisms, there are also several bilateral and minilateral initiatives launched by some allies to foster cooperation in EDTs, for example the US-led AI Partnership for Defense, which brings together about a dozen allies and partners, and the US-UK Artificial Intelligence Cooperation Statement of Intent. These initiatives, however, approach EDTs differently. The EU generally follows a more restrictive approach. The EU Parliament has for example called several times already for a ban of autonomous weapon systems and also the EDF's resources are not supposed to be used for autonomous weapons systems that lack meaningful human control.

To prevent further fragmentation and duplication as well as double-standards, the priority should now be to foster greater cooperation, harmonization and coherence between the different initiatives and mechanisms.

Bernardo Navazo

As one could read between lines in my previous answer, when I look at NATO I see two different political communities (the US and the EU) that share enough security interests so as to fuel a Transatlantic security organization. But that does not mean that both communities share all of its interests in the widest array of topics nor that we think the same when it comes to the greatest challenge of this XXI century, which is how to interact with China.

As a European, achieving our strategic autonomy to the greatest possible degree is a must for our political community. That entails finding our own voice in global discussions and having the means to both defend ourselves (territorial integrity and political sovereignty) and project our interests. The term "a Geopolitical Europe" points into that direction, and it is a trend that I foresee has arrived to stay. To that end, we are building our own supply chain of microchips and semiconductors, hydrogen, batteries, renewable technologies, vaccines, and the like.

European defense is a tricky issue, for we inherit dynamics coming from the post-WW2 security system (under Washington aegis) in which the US was the ultimate security guarantor. It is difficult to see that the European hegemons (Germany and France) would take over that role when it comes to protecting the EU anytime soon. In this impasse the EU and its Member States oscillates between the search for more strategic autonomy (building European military capabilities, promoting European defense industries) and the falling back on our all-time ally.

Regarding the technological dimension, what synergies should be promoted between the Common Security and Defense Policy (CSDP) of the European Union and the new NATO Strategic Concept?

On the other hand, many American IR scholars agree that the US cannot make "credible commitments" when it comes to the European theater. Washington's priorities are only two: to rebuild its economy and to deter/counter China. If Brussels does not go along with Washington's request to counter Beijing, would Washington still maintain its security commitments vis-à-vis the EU? Let's add the prospect of more nativist politicians winning the US mid-term elections or the 2024 Presidential election and the validity of NATO Art. 5 become dubious. I believe French and German policymakers have that in mind.

That said, the best cooperation between NATO and the CSDP (or between the EU and the US, if you look at if from my perspective) is the one that could resist the stress test of a potential 2024 Trump victory. Believe the claims of more public commitments by Washington on military and security issues in the European theater and a 2024 nativist US President would prove you wrong. On the other side, focus on areas in which a more nativist US and the EU still share interests and the ensuing NATO will survive.

Which areas are those? Some come to my mind: technology and science monitoring (as developed in the previous questions), global freedom of navigation, fight against climate change,... European security is no longer a value shared by a more nativist US, and the EU and its CSDP are to take that into account.

"The most obvious and impactful synergy is focused on advancing technological developments that align with democratic principles–protecting privacy, civil and human rights, and rejecting the use of technology for repression and to perpetuate authoritarian modes of governance and rule."

- Margarita Konaev

KEY TAKEAWAYS

PANEL 2

Ukraine, NATO enlargement and military technologies: A turning point in the security architecture

So far, 2022 has not been an optimistic year as far as geopolitics is concerned. With the war breaking out in Ukraine in February, countries worldwide gave their security structures another thought. Finland and Sweden were quick to apply for NATO membership, putting them on a fast track to join the security umbrella under the Alliance. The conflict also prompted a turning point in the use of military technologies, both for good and to cause harm. On the one hand, private actors and companies rapidly provided network connectivity, cyber tools and facial recognition technology to identify enemy assailants and those deceased in combat. On the other, the use of autonomous weapons, spread of disinformation campaigns and cyber-attacks on critical infrastructure caused more damage than ever, leading to an escalation of conflict that continues to this day.

These were the topics addressed during the second panel, moderated by **Paula Martínez**, Research Project Coordinator, Center for the Governance of Change

PANELISTS

Jeremy Cliffe

International Editor, The New Statesman

Olga Tokariuk

Independent Journalist and Non-Resident Fellow,
Center for European Policy Analysis (CEPA)

Oscar Jonsson

Director, Phronesis Analysis and Researcher,
Swedish Defense University

Paula Álvarez-Couceiro

Associate Director, IE School of Global and Public Affairs

ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

NATO OTAN

What scenarios of evolving aggression against Ukraine do you foresee?

Jeremy Cliffe

I think of the war in terms of three main scenarios. In the first, Russia is pushed back to (or close to) the borders before 24 February and the invasion is a clear failure and humiliation. This might be accompanied by turmoil in Moscow and potentially even Vladimir Putin leaving the presidency. In the second scenario, Russian troops manage a "breakthrough"; overwhelming exhausted Ukrainian forces, extending their invasion to Kyiv and ultimately toppling the Ukrainian government in line with the original objectives of the invasion. The third scenario lies between the two. Here, Russia takes much of the Donbas but an artillery-centric conflict continues along a long line running through eastern and southern Ukraine for a prolonged period lasting well into 2023 and perhaps even 2024. It goes through periods of greater and lesser intensity and becomes a long-term feature of the European landscape - at the cost of appalling suffering by the Ukrainian people and extended instability for the continent as a whole.

I consider this third scenario, of prolonged regional conflict, the most likely of the three. And that is worrying. The quality of Russian strategists, troops and technology is clearly much lower than many feared when the invasion started. But Ukraine's impressive resistance requires strong support from its Western allies. Yet the longer the conflict lasts, the greater the risk of "war fatigue" among them. Already debates in Western European capitals are turning to cost-of-living and energy crises facing domestic populations. And then there is the potentially transformative possibility of a new Trump (or Trump-like) presidency in the US at the 2024 election there. It is not at all surprising that President Zelensky reportedly wants a rapid conclusion to the walk. Putin has time on his side.

Olga Tokariuk

First, I envision a full-fledged attack from the territory of Belarus, involving Belarusian army (currently only territory and military bases in Belarus are used for attacks on Ukraine, but not Belarusian personnel), again targeting Kyiv and northern part of Ukraine: the goal would be to capture the capital, but also distract Ukrainian resources from the east and south of the country.

Second, if Russia seizes more Ukrainian territory in Donbas, it will station its military hardware there and use it as a launching ground for further offensives on the rest of Ukrainian territory. Russia is already launching missile and artillery strikes from the occupied territory in southern Ukrainian Kherson region – among other places, on the city of Mykolayiv, trying to secure ground access to Odessa, in accordance with its stated goal to establish a land corridor to Transnistria and to cut Ukraine's access to the Black Sea.

Third, the potential use of chemical and biological weapons.

Fourth, a possible tactical nuclear strike against Ukraine is not excluded, although the likelihood is low at the moment and Russian threats look like more nuclear blackmail.

The situation is very fluid though, there is nothing pre-determined. The agency and determination of Ukrainians to resist and to make their country survive should be taken into account. What happens next will depend very much on how fast Ukrainian armed forces will receive weapons promised by the Western partners, and which ones exactly to alter the situation on the ground. There is still a lot of room for maneuver for both sides, despite recent Ukrainian retreats from Donbas.

With sufficient amounts of weaponry, first of all heavy artillery, it is highly likely Ukrainians will be able to launch successful counterattacks and liberate at least some territories, occupied by

What scenarios of evolving aggression against Ukraine do you foresee?

Russia since February 24. Then new variables, such as Russian response (with a possible use of non-conventional weapons), come into play. But much will depend on the West and NATO reaction and their continued resolve to support Ukraine with weapons, training and intelligence.

Once the war is over, the issue of future security guarantees for Ukraine should be on the agenda. How to prevent Russia from further invasions? The only answer I have now is that Ukraine should be integrated into Western security architecture, including NATO. After Russia's brutal invasion, it is increasingly obvious – and not just to Ukraine - that there are only two viable options for a country to feel safe from aggression: be a member of a collective security alliance or have a nuclear deterrent.

Oscar Jonsson

While July seems to be a period of an operational pause on the Russian side, Russian maximalist goals are still there and do not seem to be changing. Moreover, the Russian side has a long history of utilizing ceasefire-agreements for their strategic benefit.

Rather, the most likely scenario is a pivot from a strategy of maneuver to a strategy of attrition. The Russian leadership are calculating on the West losing their interest and ability in financially and militarily supporting Ukraine. Similarly, Western leaders are banking on that their sanctions will hurt Russia so much that it will cave in. Time will tell.

Paula Álvarez-Couceiro

The conflict in Ukraine is entering a new phase. The first phase constituted a special mission to take Kyiv with the intent of removing the current government and creating a Russian puppet regime like in Belarus. After a poorly executed campaign, the Russian military recalibrated and set their new objective in taking eastern and southern Ukraine and further securing the Donetsk, Luhansk, and Crimean regions originally invaded in 2014.

The summer months constitute a point of inflection where both sides have to adjust their strategy yet again. As it stands right now, in early July 2022, the Russian military has instituted an operational pause intended to give Russian troops time to regroup and rest. The war seems to be moving into a war of attrition, as gains continue to be limited and there are increased personnel losses with limited reinforcements.

If this is the case, the Russian military is much more likely to endure this type of fight given the size of their military and the fact that it is a type of conflict they are comfortable fighting. On the other hand, the Ukrainian military should shift their strategy from a defensive fight to an offensive fight to take back lost territory. However, offensive battles are considerably harder to fight and Ukrainian frontline positions currently lack sufficient weapons and ammunition as Western supplies are slower to arrive on the frontlines.

Overall, the autumn months will showcase much more limited territorial changes on either side, combined with continued heavy artillery fire and increased personnel losses, leading to increasingly hollowed out militaries which will be harder to maintain unless massive conscription and training is constituted soon.

How has hybrid warfare evolved in the aggression and what role will cyber and disinformation play in the changing nature of international conflict?

Jeremy Cliffe

Clearly the most significant example of hybrid warfare in the conflict so far has been the Russian blockade of Ukrainian Black Sea ports, preventing the export of grain and fertilizer crucial to global nutritional supply chains. Putin's goal is clear: to stir up chaos in a way that pushes Western governments to seek a rapid conclusion to the conflict even at Ukraine's expense. The blockade is driving up global food prices, which serves that goal, but will have a particularly acute effect in certain fragile societies in Europe's near-abroad. Of particular concern are Egypt and Ethiopia, with their large populations and major strategic significance (the first a Western security ally perched on the crucial Suez Canal chokepoint, the second given its dominant position on the Horn of Africa). Mass famine in such countries will mean new migration crises and associated chaos in Europe and globally.

Inevitably, the role of cyber and disinformation in conflict will only grow. The question is how countries adapt to them. Here, a good example from which to learn is Estonia. The small Baltic state experienced a massive Russian cyber attack in 2007 and with its Russian-speaking minority is a prime candidate for disinformation and other provocative hybrid interventions. Yet it is a great example of how to build resilience in the face of such threats. Estonia has made itself a global leader on cyber defense. And it goes to special efforts to make its population robust in the face of disinformation and other influence operations; courses in media and information literacy are now a fundamental part of school curricula. Strong, cohesive, open and well-prepared societies are the best shield against hybrid warfare and Estonia is a great illustration of that fact.

Olga Tokariuk

Russian cyberattacks on Ukraine have largely been thwarted and didn't cause substantial damage (also thanks to tremendous work by Ukraine's ministry of digital transformation that managed to transfer crucial data to external servers in anticipation of the invasion), but there is still a possibility of new and more damaging ones.

Ukrainian military on the ground report that Starlink internet terminals play a crucial role in securing stable communications between Ukrainian armed forces in the East and help to save many lives.

We can expect Russian disinformation and propaganda efforts against Ukraine to continue and intensify, especially as media presence on the ground in Ukraine shrinks and the media coverage of the war slowly fades away. Russia will use this to fabricate fake stories from Ukraine to discredit its armed forces, government, civilian resistance and humanitarian effort (expect something along the lines of the White Helmets smear campaign in Syria).

As the global food crisis exacerbates, global fuel prices and inflation rise, and winter approaches, Russia and its assets worldwide will try to 'internationalize' the conflict: increasingly blame Ukraine for global problems, in an attempt to erode support for Kyiv. This will very likely find sympathy among the audiences in the Global South, where Russian propaganda has been quite efficient and which will suffer the most from food crisis and rising prices, but also among the populations of European countries, heavily reliant on Russian gas.

In this context, it is especially important to constantly remind the public that it is Russia who is primarily responsible for the global food crisis, because of its blockade of Ukrainian ports which prevents Ukraine from exporting its grain worldwide.

How has hybrid warfare evolved in the aggression and what role will cyber and disinformation play in the changing nature of international conflict?

It should be expected as well that the Russian propaganda machine will try to further sow divisions in the West by amplifying threats of new migration waves to Europe and the USA due to the food crisis and deteriorating economic situation in the Global South.

Oscar Jonsson

The 2022 Invasion of Ukraine is a reminder that "hybrid warfare" is not a catchall for competition in the 21st century. Rather, it was perceived to be successful in the 2014 invasion of Ukraine with the annexation of Crimea. This relied on a combination of military means with a number of non-military means (disinformation, intelligence operations, bribery and cyberattacks).

However, it is important to remember that it was successful in very unique circumstances. On the one hand, you had the leadership vacuum in Ukraine with the plight of Yanukovych, but on the other hand you had Western powers and NATO unwilling to do something. This enabled Russia to conduct "hybrid warfare" in a time of genuine confusion in Ukraine which lowered their determination at the time. Simultaneously, Western power were also enabling Russian aggression by acting confused and not stating what was happening.

By comparison, Russian information warfare against the West has in 2022 largely been unsuccessful. The latest invasion was so blatant that it provided no degree of ambiguity or deniability of who was the aggressor. This serves as one reminder of the context-specific nature of the tools applied in competition and warfare.

Paula Álvarez-Couceiro

Hybrid warfare has evolved into a concept we identify as imperceptible and untouchable and we have the perception it is new in the era of technological advancements. In fact, activities below the threshold of war have existed since the beginning of time. New technologies facilitate disruption and accelerate its pace, but it is not a new concept. Hybrid warfare should be thought of as a preparation of the field for war, an attempt to weaken the adversary ahead of the fight, a means to an end. The Russian Federation is particularly prone to the use of hybrid warfare in this way, as can be seen through the denial of service (DDOS) attacks on Georgia before Russian invasion in 2008, the repeated cyber weapons used on Ukraine before the 2014 invasion, which have continued ever since, and a long list of other examples throughout its history.

Similarly, the Soviet Union used disinformation since its inception and has continued to do so. The recent book Active Measures by Thomas Rid provides a historical account of disinformation efforts by the United States and the Soviet Union since the early 20th century.
Western nations should do a better job of demystifying hybrid warfare as an unknown and unforeseen challenge and educate the general public on the changing nature of hybrid threats and its expansion into the sphere of the general public as facilitated by technological development.

How much emphasis should NATO place on the current threat to Europe from Russia versus the more systemic challenge posed by the strategic rise of China?

Jeremy Cliffe

This question gets at a major ongoing debate in strategic circles: does Russia's attempt to invade and subordinate Ukraine tell us things that should shape our China policies, or is it a largely or wholly irrelevant precedent where they are concerned? I consider the latter of these a reasonable position. China has a stake in a stable international environment in the way that Russia does not, especially given its growing internal problems (a crisis-hit property market, dangerous debt levels, divisive Covid policies, a fast-aging population, the so-called middle income trap). But fundamentally I tend more to the former position. Xi Jinping has made it clear that he sees the "return" (conquest) of Taiwan as a significant Chinese goal, in a way that recalls Putin's vision of Ukraine in certain respects and might see China's leadership to draw lessons from the West's response to the Russian invasion. The country is fundamentally a revisionist power in the way that Putin's Russia is too. And the West has long been complacent and naive in its dealings with Beijing, just as it was for many years in its dealings with Moscow. China is not Russia, Xi is not Putin. But there are significant parallels that should worry us.

So: it is hard to separate the two. The West does need to put up a credible response to Russia now, and it needs to engage in the systemic contest with China. But really this is not an "either/or" choice. It has to manage both. Combined with the West's own internal challenges, that is no mean feat.

Olga Tokariuk

Russia and China are two issues that cannot be fully separated. It is impossible to focus on countering the strategic rise of China – peaceful for a time being – without countering belligerent and increasingly aggressive Russia. The outcome of war in Ukraine will define China's further actions in what it considers its own 'sphere of influence' such as Taiwan. Beijing is watching closely how the West responds to Russia's attempt to crush a democratic and sovereign state.

For now, defeating Russia in Ukraine and deterring its further aggression in Europe should be a number one priority. Russia is increasingly threatening Lithuania over its decision – in compliance with the EU sanctions – to prevent rail transit to its exclave of Kaliningrad. If Putin feels that he is not stopped in Ukraine and can get away with the war crimes the Russian army committed there, he will feel emboldened to attack a NATO country - and the Baltic states would be his primary targets. This would be a definite end of the post-WWII international order and will likely lead to the new global conflict.

China is tacitly supporting Russia's war on Ukraine, and this should be kept in mind when defining future strategies. The West's and NATO credibility and global balance of power are at stake.

What the West could do now is to start decreasing its economic dependency on China, however painful that may be.

How much emphasis should NATO place on the current threat to Europe from Russia versus the more systemic challenge posed by the strategic rise of China?

Oscar Jonsson

While the challenge from China is significant, very little of it should be handled by NATO. NATO was founded as an alliance for the territorial defense of European and Northern American states. The key for handling China today is more focused on things that are outside NATO's tasks: trade, technology and economy statecraft, as well as diplomacy.

As long as NATO's European states would be unable to fight an artillery war of the type in Ukraine, they should fix that rather than thinking about threats on the other side of the globe. NATO's focus on China is of course driven by the US, but the most useful thing that NATO's European states could do to support the US in China is taking a bigger burden of European security away from the US.

Paula Álvarez-Couceiro

The 2022 NATO Strategic Concept is clear in designating China as a 'systemic challenge' but prioritizing Russia as 'the most significant and direct threat to Allies' security'. NATO continues to be a transatlantic defensive alliance and, while it should consider the challenges posed by China, it should not lose sight of its ultimate purpose of safeguarding the transatlantic members from the threats posed by Russia.

If NATO were to designate China as an adversary, it should be ready to create a clear military strategy to address the threat and ensure its military capabilities can be divided between two theaters, Europe and the Indo-Pacific. If NATO is not ready to defend both theaters militarily, then it should not go further in designating China as an adversary.

Nonetheless, the 2022 NATO Summit incorporated Asia-Pacific partners for the first time. The Madrid Summit provided an important venue to showcase solidarity between partners, while understanding that each partner will favor taking military action in the regions closer to their borders.

CONCLUDING REMARKS

Manuel Muñiz

Provost, IE University

We live in very interesting times. Over the last year, the geopolitical context of Europe has witnessed a radical shift, and technology has played a large role in this.

Just as climate proved the need for "climate diplomacy" or breaking the perception that the environment constituted a very technical field that lay in the hands of scientists alone, technology follows the same direction.

Technology has a strong power dimension with the gradual adjustment of offensive and defensive capabilities by sovereign nations, the development of new and emerging threats in cyber and outer space.

With this change of scenario in the global arena, there is an increasing urge to prepare for the future. It is therefore necessary to train the new generations of diplomats and policymakers in these topics, and where schools of Global and Public Affairs, such as ours at IE University, or others such as Sciences Po or LSE, play a huge role in providing this academic training.

The Safer Tomorrow: Security starts with YOU(TH) initiative aims to take advantage of changing global dynamics. It will mobilize students and faculty across institutions and bring their ideas into the reflection on how to reconstruct the global security architecture that is currently under review.

To enact change, it is pivotal to engage in partnerships with key actors in the field. We are honored to join forces with the NATO Public Diplomacy Division and advance this initiative side to side.

As Former Minister of Foreign Affairs of Spain and my good friend Arancha González Laya put it, "security and defense matter for all of us, and we need the involvement of the younger generations to prepare for what is to come."

I look forward to seeing what this initiative can achieve in raising awareness and creating a safer tomorrow.


ie
UNIVERSITY
CENTER FOR THE
GOVERNANCE OF
CHANGE


NATO
OTAN