https://doi.org/10.70265/YIAM8555

EU-NATO COOPERATION AND INNOVATION IN EMERGING DISRUPTIVE TECHNOLOGIES TO STOP RUSSIAN-CHINESE HYBRID WARFARE IN THE ENERGY TRANSITION

Maurizio Geri

Summary: *How can the EU and NATO face the future hybrid threats coming from Russia and other adversaries like China in the energy sector during the green transition? Energy security is among the most vulnerable sectors of national security, with significant potential to destabilize societies. Both the green energy and technological transitions will increase vulnerabilities of new infrastructures, supply chain and technologies in the decades to come. The West therefore will need a grand strategy, to increase resilience and capabilities investing in innovation for new technologies (so called "Emerging Disruptive Technologies"/EDTs), defending the supply and value chain of critical materials and resources, and protect the new infrastructures. A closer and more efficient cooperation between the EU and NATO in these sectors becomes fundamental, as dual use technology could help in both the technological and energy transitions and hinder new non-kinetic warfare in these areas.*

Key words: *Hybrid Warfare, Energy Security, Emerging Disruptive Technologies (EDTs), EU-NATO Cooperation, Supply Chain Resilience*

INTRODUCTION

A new GPC in energy security and technological transition

History is master of life as Cicero said, and two history lessons are particularly relevant today.

The first is the one that British economic historian Maddison explained (Maddison, 2005): the dominant global power of each era is shaped by its technological progress, as seen with the Netherlands in the 17th century, the UK in the 19th, and the US in the 20th. As modern scholars argue (Calcara et al., n.d.) power is about more than just a big army or strong economy: those who bet on technological innovation can win also today the great powers competition (Schmidt, 2023). The second important lesson of our recent history, is that in the past century, the two major anti-Western alliances – the Axis powers in WWII and the Communist bloc in the Cold War – viewed the West as an oppressive imperial system hindering their own ambitions, but they lacked a unified strategy as they had mutual distrust.

Today's Axis of Upheaval (Kendall-Taylor, & Fontaine, 2024) with China, Russia, Iran, and North Korea are similar as their leaders regard themselves as world-historical men of destiny. But there is a difference: they started working closely in defense-industrial cooperation, to prepare for a period of major confrontation (Zelikow, 2024). The West therefore need a new 'grand strategy' to deal with that.

Technology is the realm of competition between democracies and dictatorships, and also today Western democratic alliances, in particular NATO and EU, are stronger alliances, value-based ones with ability to create new unified strategies because of skills of adaptation and resilience, typical of democracies. But there is no guarantee that we will not go towards a systemic war between West and East, as the assumption of the West, that its rivals will act rationally, without risking violent escalation, has been debunked over and over, as we saw with Russia and Iran recently. Therefore, to avoid escalation towards kinetic warfare the West need to win the non-kinetic part of what we call "hybrid warfare" (Hoffman, 2007), in particular the technological and energy warfare.

The disruptive potential of new technologies and the energy transition are among the most vulnerable arenas for exploitation in hybrid warfare (Tech Accord, 2022). To say it with former CEO and chair of Google, Eric Schmidt, "technology will define the future of geopolitics" (Schmidt, 2023) with the new "Tech Wars" (Gerstein, 2022) and the industrial policy of tech the "next geopolitical great game" (Gili & Tentori, 2023). According to the International Energy Agency (IEA) the 75 % of the technologies needed to achieve net zero are yet to be invented. Just 25% of the emission cuts needed to meet net-zero can be achieved by mature technologies, such as wind, solar, nuclear; 41 % will have to be addressed by technologies currently at the early adoption phase, and 32 % by technologies still at a prototype phase (IEA, 2021a).

In the next decades who will tackle energy and technological transition with primacy will therefore win the final great powers global competition. The West has still advantages until now in these areas because of its three fundamental skills: ability of adaptation and resilience, investment in innovation, and fostering new alliances (Karp & Maass, 2024), but is not sure it will keep them in the future, as Russia and China are growing in all the three areas, so the West needs a new unified strategy. The playground for this strategy is the new energy and resources security nexus, where there is an increasing application of non-kinetic hybrid threats, from attacks to power grids and gas distribution, to disruption of supply chain.

The US is still the leading technological power today: nine of the top ten technology companies are American, and if US dominates the technologies of the present, could also lead the industries of the future, such as AI and bioengineering. But is not a given, also, because the EU is not

supporting the US very much in high level competition in these areas, and the US alone cannot make it if the West is not unified. The recent EU report by Draghi (European Commission, 2024) in fact shows that the EU has an existential threat, as it has slow growth and low investment in innovation and competitiveness. For instance, the EU's share of global R&D spending remains significantly lower than that of the US and China, with fragmented investment structures and slow policy implementations further compounding the issue. To become a leader in tech, climate responsibility, and a player on the world stage, the EU needs investment to rise by 5% of GDP, something like 3 Marshall Plans[1], involving all the civil forces of our societies. In fact, as experts argue (Calcara, 2023) the optimal way to generate innovation is to create open ecosystems between large corporations, small firms, start-ups, open-source communities and end-users. Which is why EU and NATO aim to develop a "triple-helix" approach to stimulating technology innovation involving the three main sectors of industry, academia and public organisations (NATO, 2020). The technological innovation and energy security during the green transition needs a new grand strategy, in what can be called the energy-resources-climate security nexus.

1. A NEW GRAND STRATEGY FOR THE ENERGY-RESOURCES-CLIMATE SECURITY NEXUS

As explained in my recent article (Geri, 2024), what we can call the "energy-resources-climate security nexus", is the connection that exists between energy security, resources need, and green transition because of climate change. The fact that green transition will make the West more vulnerable to new hybrid warfare in the energy sector, because of new technologies, infrastructures and supply-value chains, creates this security nexus. Therefore, the West will need a new "grand strategy" to deal with it, to deter, defend and react to new types of hybrid attacks. In general, a grand strategy is based on the "whole of government" approach, using different tools that can be included in acronyms like PMESII (Political, Military, Economic, Social, Information, Infrastructure) PESTLE (Political, Economic, Social, Technological, Legal and Environmental) or DIMEFIL (Diplomatic, Informational, Military, Economic, Financial, Intelligence, and Law Enforcement) (AU Library, 2024). Whatever acronym we use a grand strategy is based on using all instrument of powers.

This article focuses on the economic, infrastructure, and technological dimensions of the energy transition, emphasizing the rising risk of hybrid

[1] The 3 areas the report identifies are: close the innovation gap with US/CH, especially in advanced technology; a joint plan for decarbonization and competitiveness; and increase security reducing dependencies. This third area in particular is important has the EU has extensive external dependencies in critical raw materials (CRMs) and advanced tech, and these dependencies could become vulnerabilities if used as "geopolitical weapons" by its rivals.

warfare from rival nations. Even if there we don't go deep in the definition of 'hybrid warfare' here, as the concept is still much debated in the academia (Bankov, 2024; Libiseller, 2023) let's say that hybrid warfare creates a state of "permanent warfare", a constant conflict with the "weaponization of everything" (Galeotti, 2022), with "subthreshold activities" (Bērziņš, 2020; Skingsley, 2020), meaning "short of (kinetic) war" strategies, tactics and operations, and with a competitive behaviour that does not necessary involve the use of lethal force. It is clear that Europe is increasingly experiencing the 'weaponization of everything' by Russia and other rivals of the Western liberal order. NATO actually sounded alarm on this increased hybridization of warfare in May 2024 over more and more hostile Russian activities in Europe (Askew, 2024) and the EU around the same time called for a firm response to counter Russian interference (European Parliament, 2024b). Russia's strategy of weaponizing of everything is evident: from the blockade on Ukraine's grain exports, to the orchestrated influx of refugees towards the Belarus-Poland border, from the removal of border markers with EU countries like the case of Estonia river, to the jamming of GPS for air transport on the Baltic Sea, to plotting sabotage across Europe (Seibt, 2024). NATO (NATO, 2024a) and the EU (European Parliament, 2024a) are therefore increasingly worried about Russian hybrid and malign actions and made several declarations of intents.

The potential for hybrid warfare in the energy transition is evident with the past Western dependence on Russian energy and also the current dependence on Chinese resources and technologies for the supply chain of the energy transition. The EU still imports 18% of its gas from Russia (Eurostat, 2024), after almost 3 years since the invasion of Ukraine. This because several countries still evade gas sanctions and the EU sanctions of last June on liquefied natural gas (LNG) are only for re-exported LNG (Borrell, 2024), showing how an energy dependency cannot be changed overnight[2]. Russian hybrid warfare or 'shadow war' in energy, targets critical infrastructures with sabotages on NATO soil (Schmitt, 2024; Pillai, 2023) but also attacks on Ukraine energy infrastructure, that is useful not only for Ukraine but also for the EU, as since March 2022, the Ukrainian electricity grid has been connected to the EU grid (Moscow's bombs have destroyed over 80 per cent of Ukrainian thermal power plants and 50 per cent of hydroelectric power plants after two years of war (United Nations, 2024)).

Therefore, it is very worried the complete EU dependency on China for its energy transition, as EU imports 80% of its solar panels and 98% of its

[2] Furthermore, since the invasion of Ukraine, European companies kept supplying equipment to Russia's LNG projects, like Arctic LNG 2 project with over USD 630 millions, despite it being under Western sanctions. The largest suppliers include Italy (EUR 112 million), France (EUR 31.6 million), Germany (EUR 25 million), and the Netherlands (EUR 12.8 million). See: Razom We Stand. (2024, June 19). *Fuelling change: Europe's battle against Russian fossil fuels*. Energy Transition. https://energytransition.org/2024/06/fuelling-change-europes-battle-against-russian-fossil-fuels/

Rare Earth Elements (REE)[3] and Critical Raw Material (CRM)[4] used in wind power generation, hydrogen storage or batteries, from China (Keßler, 2024). REEs and CRMs are therefore very economically significant and vulnerable to possible supply disruptions (U.S. Department of Energy, 2023). Furthermore, China uses unfair government subsidies for goods needed for the green transition, like the electric vehicles, flooding in this way the European market and creating another area of dependency. Which is why recently the EU adopted a CRM act[5], started high tariffs on EVs (Reinsch & Whitney, 2024) and a de-risking strategy even if not yet de-coupling (Brinza et al., 2024).

This dependency of the supply chain is coupled with the new cyber vulnerabilities of energy infrastructures (Finley, 2024), already target of cyberwarfare from Russia and Iran (Lopez-Rodriguez, Moreno-Lopez, & Hernández-Gutiérrez, 2023; Cassetta, 2024) or anyway Russian and Iranian criminal groups (Stoddart, 2024), but could be under threat from China soon too. And the technological element is very much related with this infrastructure element and supply chain, as the new infrastructures will be more and more impacted by the emerging technologies and the competition on REEs among great powers too.

The International Energy Agency for example predicts that by 2040, demand for REEs could surge three to seven times their current levels and mineral demand for use in EVs and battery storage should grow at least thirty times to 2040 (IEA, 2021b). China accounted for 70% of the world's mine production of rare earths in 2022 (Textor, 2024), followed by the US, Australia, Myanmar, and Thailand. Nevertheless, as with the game changing fracking technology in US that made the US the number one producer of oil

[3] REEs comprise 17 elements play a critical role to energy independence. Many technologies have components made from REEs such as magnets, batteries, phosphors, and catalysts. Info retrieved from Conrad, R. (n.d.). *Rare Earth Elements*. U.S. Department of Energy. https://www.energy.gov/fecm/rare-earth-elements; and European Commission. (n.d.). *Rare earth elements, permanent magnets, and motors*. Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/rare-earth-elements-permanent-magnets-and-motors_en. Energy critical elements (ECEs) are elements integral to advanced energy production, transmission, and storage. This category includes lithium, cobalt, selenium, silicon, tellurium, indium, and REEs. Information retrieved from Center for Sustainable Systems. (2024). *Critical Materials Factsheet. (Pub. No. CSS14-15)*. University of Michigan. https://css.umich.edu/publications/factsheets/material-resources/critical-materials-factsheet

[4] CRM are materials of high economic importance for the EU and US, with a high risk of supply disruption due to their concentration of sources and lack of good, affordable substitutes. European Council and Council of the EU. (2024, September 12). *An EU critical raw materials act for the future of EU supply chains*. https://www.consilium.europa.eu/en/infographics/critical-raw-materials/; and Critical Materials Institute. (n.d.). *Critical Materials Institute an Energy Innovation Hub* [PowerPoint slides]. U.S. Department of Energy. https://www.energy.gov/sites/prod/files/2014/06/f17/Critical%20Materials%20Institute.pdf

[5] In March 2024, the Council of EU adopted the European critical raw materials act, to secure a sustainable supply of critical raw materials, enabling Europe to meet its 2030 and 2050 climate and digital objectives, as demand for REEs is expected to increase exponentially in the coming years. European Council and Council of the EU. (2024, September 12). *An EU critical raw materials act for the future of EU supply chains*. https://www.consilium.europa.eu/en/infographics/critical-raw-materials/

on the planet, the US, Europe, and other allied states could discover new mines of REEs or invent new technologies that will allow us to have more efficiency and avoid the dependency on REEs. Which is why investment in innovation becomes crucial, in particular in dual use military/civilian technologies.

Therefore, how we control Western vulnerabilities for next decades, in particular on most vulnerable NATO and EU countries and their civil societies? How we make sure to deter and defend from attacks on critical infrastructure, secure the supply chain, and win the technological innovation not only for national security but for homeland security of our civil societies (actually one of the seven NATO requirements for civil preparedness is "resilient energy supplies" (NATO, 2024d))? How we make sure for example that electrifying everything, from water pipelines to cars, we are not increasing vulnerability to cyber attacks? Or how do we build the technology that we need – innovative, sustainable, adaptable, secure, and at the huge scale needed for future energy security? We are in an energy security dilemma (Tang, 2009) (like traditional security dilemma): who we chose as partners and which technologies and infrastructures we build will be crucial. We need a new energy security strategy.

The new strategy will need to make the supply and value chain of critical materials independent with diversification, defend vulnerable critical infrastructures and innovate in new technologies. In one word the new strategy should give resilience to the West, meaning the ability to deter, detect, withstand, and recover from hybrid attacks against energy security. The three pillars of this new strategy should be:

- **Guarantee the security, sustainability and affordability (the "energy trilemma") of the supply chain** for REE/CRM in the future competition. The resource scarcity and geopolitical disruptions will threaten our supply and value chains, so it is fundamental to have them protected and guaranteed through diversification and de-risking from rivals.

- **Defend critical infrastructures**, as infrastructures are increasingly target of physical and cyber hybrid warfare, so it is fundamental to protect them, especially with the energy transition that might make infrastructures more fragile and vulnerable, especially the new infrastructures underwater (Cassetta, 2024).

- **Invest in dual use innovative technologies, the so called Emerging Disruptive Technologies** (EDTs) as defined by NATO (NATO, 2024c), in particular AI, autonomous systems and quantum technologies. Civil-military lines are fading, civilians' assets are increasingly used for military purposes and the opposite too, therefore dual use technology will be the arena of future competition for both civilian and military purposes.

This article as said, focuses in particular on how to improve the cooperation between the two strongest and longest alliances of the West,

NATO and EU, to invest in dual use EDTs and energy security, in this way increasing resilience and capabilities, avoiding vulnerabilities to be exploited in new hybrid warfare and win the final competition with its rivals.

2. A NEW NATO-EU COOPERATION IN HYBRID WARFARE AND TECHNOLOGY

To win the competition and possible new hybrid warfare in the 'energy-resources-climate security nexus' we need NATO and EU to increase cooperation in hybrid warfare, technology and energy security.

The EU and NATO have been late, respect to Russia, in the operationalizing of the concept of hybrid warfare, especially in energy, and also on the strategies to deter and defend from it. The EU developed a 'Joint Framework on Countering Hybrid Threats' only in 2016 (European Commission, 2016) and NATO stated that hybrid actions against a member of the Alliance could lead to the invocation of Article 5 of the Treaty the same year, 2016 (NATO, 2024b). But it has not been until July 2022 that NATO Leaders endorsed comprehensive preventive and response options to counter hybrid threats, and NATO's Joint Intelligence and Security Division created a hybrid analysis branch to improve situational awareness (Ruhle, & Roberts, 2021). In recent years (NATO, 2023a), NATO and EU increased cooperation in the European Centre of Excellence for Countering Hybrid Threats (created in 2017 in Finland), and between the NATO Joint Intelligence and Security Division Hybrid Analysis Branch and the EU INTCEN Hybrid Fusion Cell, with the aim of strengthening situational awareness. So, NATO and EU are currently increasing their response to hybrid warfare and their engagement in this arena (NATO, 2021; Kols, 2018) but according to some scholars the Alliance is not yet prepared for these "subthreshold" threats (Polyakova et al., 2023) and still a lot can be done, especially in the energy sector. Actually, among the non-kinetic tools, Russia has been particularly keen to weaponize the use of energy (Balmaceda, Greene, Schmitt, Kluge, & Pavlenko, 2023), given the European energy dependency.

At technological level, NATO and the EU also need to step up their cooperation, in particular in the dual use technology to fight the new vulnerabilities and leverage collective technological development in particular for energy security like protection of critical infrastructures. The need for NATO and the EU to cooperate more in dual use, defense and civilian, technology is clear (Speranza, & Jens, 2021), also because NATO's commitment to deterrence and defence requires a coordinated defence industry among its members (Polyakova et al., 2023), which is why also NATO created recently a Defense Industrial Production Plan (NATO, 2023c).

One of the problems is that the EU is still behind US and China in technological innovation, which has become a crucial tool of power competition. The already cited EU report on "The future of European competitiveness" by Mario Draghi, identifies three urgent needs: to close the innovation gap with US and China in advanced tech; to make a joint plan for decarbonization and competitiveness; and to increase security reducing dependencies from critical materials and advance technologies. This last point is crucial to fight hybridization of warfare in energy sector not only from Russia but also from China.

Data from European Defence Agency shows that in 2022 EU member states only spent €3.5 billion on Research and Technology (R&T) (European Defence Agency, 2023) that is the applied branch of Research & Development (R&D) to innovation in industrial practices. By contrast, the US Department of Defence spent $34 billion on defence technology innovation in 2022, or 4% of its defence budget. The EU therefore needs to innovate more if it wants to be competitive and propose a new 'strategic responsibility' for the European continent inside NATO. Actually, triggered by the European Defence Fund, in 2022 the EU launched a Defence Innovation Scheme (EUDIS) (European Union, n.d.) with a total funding of €2 billion through 2027, to invest in Research, Technology, Development and Innovation, and to lower barriers of entry into the defence domain for smaller or non-traditional market players. But more needs to be done.

NATO has among its bodies the Science and Technology Organization (STO), that aim to maintain NATO scientific and technological advantage, providing scientific innovation and solutions. NATO STO has focused recently on nine technology areas (the EDTs): AI, autonomous systems, quantum technologies, biotechnologies and human enhancement, hypersonic systems, space technology, novel materials and manufacturing, energy and propulsion, and next-generation communications networks (NATO, 2024c). NATO has also stated to collaborate with academia, civil society, and businesses to foster public-private partnerships in technology development. Some scholars actually argue that the private sector role in warfare can represent a "sixth domain" (Kramer, 2023) (complementary to the five warfare domains of air, land, naval, cyber, and space).

NATO also has Centres of Excellence (COEs) like the Maritime Centre for the Security of Critical Undersea Infrastructure just opened in UK; a Climate Change and Security COE just opened in Canada; a Space COE in France; a Strategic Communications COE in Latvia; a Cooperative Cyber Defence COE in Estonia; and an Energy Security COE in Lithuania. Sweden has ALSO a proposition of opening a new COE on "Supply Chain Security", for the energy transition supply chain.

Furthermore, NATO has an Industrial Advisory Group (NIAG), a high level consultative and advisory entity comprising senior industrial leaders

from NATO member nations. Operating under the auspices of the Conference of National Armaments Directors (CNAD), its primary objectives include facilitating exchange of insights pertaining to industrial, technical, economic, managerial, and other crucial aspects of research, development, and production of armament equipment within the Alliance. Also, as part of the NATO 2030 agenda, NATO created in 2021 the Defence Innovation Accelerator for the North Atlantic (DIANA). The goal is to outreach to the entrepreneurs and the scientists, the human capital within NATO countries, that have ideas for news technologies that we can accelerate for both national and economic security. Dual-use technology, is having a large impact on capabilities very quickly, so DIANA will try to make these technologies more agile and apply to security programs that are different than armaments programs, like energy security, resources security, cyber security etc.

Regarding funds, NATO is funded through direct and indirect contributions of its members. National (or indirect) contributions are the largest component of NATO funding and are made by individual member countries. NATO's direct contributions to collective budgets (common funds) are around 0.3% of total Allied defence spending (EUR 3.3 billion for 2023) (NATO, 2024f). But besides common funding, NATO has joint funding when there is a need for a long-term engagement for large-scale requirements or specific initiatives. The most recent joint funding initiative is exactly the creation of DIANA. NATO also opened recently an Innovation fund, among 24 members, with 1 billion Euros that is the world's first multi sovereign fund, limited partnership for security, to invests in deep tech companies, as the talents in STEM of NATO members are world-leading, but the market to support innovation is still underfunded (NATO, 2023b). The EU should follow similar paths.

So how NATO and EU are expanding their cooperation in the technology sector, to have better deterrence and defence, especially the hybrid arena? Recent efforts have been made to enhance NATO-EU staff to staff contacts in the realm of R&D and R&T. These efforts aim at fostering mutual awareness regarding initiatives related to EDTs as well as innovation. New efforts are being made through staff-to-staff contact also to have more coherence among various NATO-EU frameworks, such as the EU Capability Development Plan, the Headline Goal Process, and the Coordinated Annual Review on Defence on one side, and on the other side the NATO Defence Planning Process and the Partnership for Peace Planning and Review Process; or between EU Defence Innovation Scheme, the Hub for EU Defence Innovation and NATO's DIANA and Innovation Fund. The objectives of all these exchanges are to identify synergies among these initiatives, but also the sharing of best practices, with a particular emphasis

on ensuring the interoperability of future solutions with existing ones (NATO, 2024e).

Regular consultations have been held also between various entities, such as the European Defence Agency and NATO STO or NATO Innovation Hub in the NATO Allied Command Transformation, to promote mutual awareness of the activities and to support complementary approaches. STO has also engaged with the European External Action Service (EEAS) and the European Commission on mutual science and technology interests, including topics like climate change, energy security, natural resources, emerging and disruptive technological challenges, and ethical considerations. Some cyber defense initiatives, like the NATO Cooperative Cyber Defence Centre of Excellence and ENISA (EU Agency for Cybersecurity) work jointly on developing best practices and conducting joint exercises. Furthermore, NATO STO Centre for Maritime Research and Experimentation (CMRE) has actively involved in maritime research projects supported by the Commission, such as project PROMENADE (NATO, 2023a).

All of these outlined engagements are beneficial but more has to be done, in particular in terms of investment in dual use technology, especially to deal with current great powers competition and hybridization of war, that will see an increasing use of EDTs.

3. RECOMMENDATIONS FOR A BETTER NATO-EU COOPERATION

NATO and EU need to identify synergies among these initiatives, but also sharing best practices, ensuring the interoperability of future solutions with existing ones, to improve technology and energy security. Future efforts should focus on:

- Make dual use technology investment a priority. To do that involve military research centres in a structured cooperation with academia and industry, to develop better dual-use EDTs.

- Enhancing public-private partnerships, to leverage the capabilities of the private sector that without public funds will not be able to develop.

- Guarantee onshore, nearshore and "friend shore" supply chains or REEs/CMRs, increasing production and process of these critical minerals, relocating them to West and friendly countries.

- Invest in R&D to develop batteries, microchips and all other technologies, reducing dependence on China's resources and manufacturing.

- Strengthening joint training programs for specialized personnel in cyber defense and critical infrastructure protection, like the recent wargaming by the Hybrid CoE of NATO and EU (Hybrid CoE, 2024).

- Advance cyber defense technologies, such as AI and blockchain, to enhance the detection and mitigation of cyber threats, facilitate predictive analytics and automated rapid threat response.

- Integrate smart grid technologies to improve the efficiency, reliability, and security of energy distribution systems, with real-time monitoring and control, reducing the risk of hybrid attacks.

- Improve critical infrastructure protection, with the implementation of advanced surveillance systems, as well as improving intelligence collaboration and unifying early warning systems.

Despite the progress made, challenges remain, including political differences, coordination complexities, and resource allocation. These are the most important challenges to prioritize and to deal with:

1. **Coordination and bureaucratic hurdles**. Effective coordination between NATO and the EU is often hindered by bureaucratic obstacles and differing operational frameworks. Streamlining processes and enhancing interoperability is essential for improved collaboration.

2. **Resource allocation**. Ensuring adequate funding and resources for joint initiatives is crucial. Both organizations must prioritize investments in cybersecurity, energy infrastructure, and technological innovations.

3. **Emerging threats**. As hybrid warfare tactics evolve, NATO and the EU must stay ahead of emerging threats. Continuous research, development, and adaptation of technologies are necessary to counter sophisticated hybrid attacks.

CONCLUSION

Russia, China are increasingly weaponizing energy resources and critical infrastructure as offensive capacities tools, in particular with attacks to critical infrastructure or material dependencies to limit the resilience of the West through economic, kinetic, and kleptocratic means. To avoid escalations to full kinetic (military) wars, therefore, is imperative to win the non-kinetic part of the so-called “hybrid warfare”. This article highlights energy as a critical sector within the economic tools of hybrid warfare, emphasizing the need for robust strategies to counter emerging threats. Effective NATO-EU collaboration is critical in countering hybrid threats. Establishing shared frameworks for energy and technological security will not only strengthen resilience but also ensure the West’s competitive edge in an evolving geopolitical landscape.

This article argued in particular that EU and NATO should cooperate more with a renewed Transatlantic approach to supporting European energy security. NATO-EU technological cooperation could play a pivotal role in countering hybrid warfare threats in the energy sector and in what can be called ‘energy-resources-climate’ security nexus. By prioritizing investing in dual use technology, critical infrastructure protection, and guarantee onshore, nearshore and “friend shore” supply chains, the West can enhance its resilience and safeguard its energy security. Continued innovation and new strategic collaborative efforts will be essential in addressing evolving

nature of hybrid warfare and ensuring the energy security of Europe and the West.

Acknowledgements

Funded by the European Union MSCA (GA number 101105349).

Disclaimer

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

BIBLIOGRAPHY:

Askew, J. (2024, May 2). *Hybrid war: NATO sounds alarm over 'hostile' Russian activity across Europe*. Euronews. Retrieved June 1, 2024, from https://www.euronews.com/2024/05/02/nato-sounds-alarm-over-russian-hybrid-activity-across-europe

AU Library. (2024, August 6). *DIMEFIL: Instruments of Power*. https://fairchild-mil.libguides.com/dimefil

Balmaceda, M., Greene, S., Schmitt, B., Kluge, J., and Pavlenko, O. (2023, March 30). *Winning Europe's Energy War with Russia*. Center for European Policy Analysis (CEPA). https://cepa.org/comprehensive-reports/winning-europes-energy-war-with-russia/

Bankov, B. (2024). Hybrid Warfare: How to Escape the Conceptual Gray-Zone. *Journal of Strategic Studies, 17*(1), 1-23. https://doi.org/10.5038/1944-0472.17.1.2118

Bērziņš, J. (2020). The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. *The Journal of Slavic Military Studies*, *33*(3), 355–380. https://doi.org/10.1080/13518046.2020.1824109

Borrell, J. (2024, June 26). *Closing the tap on Russian gas re-exports*. European Union External Action. https://www.eeas.europa.eu/eeas/closing-tap-russian-gas-re-exports_en

Brinza, A., Bērziņa-Čerenkova, U. A., Le Corre, P., Seaman, J., Turcsányi, R., & Vladisavljev, S. (2024, March 26). *EU-China relations: De-risking or de-coupling − the future of the EU strategy towards China*. European Parliament, Policy Department for External Relations.

Calcara, A. (2023, March 3). *One Step Back, Two Steps Forward: the EU, NATO and Emerging and Disruptive Technologies (CSDS Policy Brief)*. Brussels School of Governance. https://www.brussels-school.be/sites/default/files/CSDS%20Policy%20brief_2307_0.pdf

Calcara, A., et al. (n.d.). *Competition in the Digital Era: Geopolitics and Technology in the XXI Century* (*EU Research Project*). Vrije Universiteit Brussel.

https://researchportal.vub.be/en/projects/competition-in-the-digital-era-technology-and-geopolitics-in-the

Cassetta, M. (2024, June 19). *How to Respond to the Emerging Threats to Critical Underwater Infrastructure at the Time of Russia's War Against Ukraine*. Istituto Affari Internazionali (IAI). https://www.iai.it/it/pubblicazioni/how-respond-emerging-threats-critical-underwater-infrastructure

Center for Sustainable Systems. (2024). *Critical Materials Factsheet. (Pub. No. CSS14-15)*. University of Michigan. https://css.umich.edu/publications/factsheets/material-resources/critical-materials-factsheet

Conrad, R. (n.d.). *Rare Earth Elements*. U.S. Department of Energy. https://www.energy.gov/fecm/rare-earth-elements

Critical Materials Institute. (n.d.). *Critical Materials Institute an Energy Innovation Hub* [PowerPoint slides]. U.S. Department of Energy. https://www.energy.gov/sites/prod/files/2014/06/f17/Critical%20Materials%20Institute.pdf

European Commission. (n.d.). *Rare earth elements, permanent magnets, and motors*. Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/rare-earth-elements-permanent-magnets-and-motors_en

European Commission. (2016, April 6). Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. (Document 52016JC0018). EUR-Lex, Publications Office of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

European Commission. (2024). *EU competitiveness: Looking ahead*. Directorate-General for Communication. https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

European Council and Council of the EU. (2024, September 12). *An EU critical raw materials act for the future of EU supply chains*. https://www.consilium.europa.eu/en/infographics/critical-raw-materials/

European Defence Agency. (2023). *Defence data 2022. Key Findings and analysis*. https://eda.europa.eu/docs/default-source/brochures/2022-eda_defencedata_web.pdf

European Parliament. (2024a). *European Parliament resolution of 8 February 2024 on Russiagate: allegations of Russian interference in the democratic processes of the European Union (2024/2548(RSP))*. Retrieved May 2, 2024, from

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0079_EN.html

European Parliament. (2024b, April 25). *MEPs call for a firm response to counter Russian interference*. News European Parliament. https://www.europarl.europa.eu/news/en/press-room/20240419IPR20542/meps-call-for-a-firm-response-to-counter-russian-interference

Eurostat. (August 2024). *EU trade with Russia – latest developments*. European Union. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU_trade_with_Russia_-_latest_developments

Finley, A. (2024, March 31). *How Green Energy Makes Us Vulnerable to Cyberattack*. Wall Street Journal. https://www.wsj.com/articles/how-green-energy-makes-us-vulnerable-to-cyberattack-electric-vehicle-china-04f803dc

Galeotti, M. (2022). *The Weaponisation of Everything. A Field Guide to the New Way of War*. Yale University Press. https://dokumen.pub/the-weaponisation-of-everything-a-field-guide-to-the-new-way-of-war-9780300265132.html

Geri, M. (2024). Understanding Russian Hybrid Warfare against Europe in the energy sector and in the future 'energy-resources-climate' security nexus. *Journal of Strategic Studies, 17*(3), 15-34. https://doi.org/10.5038/1944-0472.17.3.2270

Gerstein, D. M. (2022). *Tech Wars: Transforming U.S. Technology Development*. Praeger.

Gili, A. and Tentori, D. (2023, December 6). *The Comeback of Industrial Policy. The Next Geopolitical Great Game*. ISPI Newsletter. https://www.ispionline.it/en/publication/the-comeback-of-industrial-policy-the-next-geopolitical-great-game-145627

Hoffman, F. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Hybrid CoE. (2024, August 28). *Wargaming courses focus on resilience of critical infrastructure*. The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/news/wargaming-courses-focus-on-resilience-of-critical-infrastructure/

IEA. (2021a). *Energy Technologies Perspectives 2020.* International Energy Agency. https://iea.blob.core.windows.net/assets/7f8aed40-89af-4348-be19-c8a67df0b9ea/Energy_Technology_Perspectives_2020_PDF.pdf

IEA. (2021b). *The Role of Critical Minerals in Clean Energy Transitions.* International Energy Agency. https://www.iea.org/reports/the-role-of-critical-minerals-in-clean-energy-transitions

Karp, R., and Maass, R. W. (2024). *Alliances and Partnerships in a Complex and Challenging Security Environment*. SACT NATO HQ. https://www.act.nato.int/wp-content/uploads/2024/06/NATO-AC24-Compendium.pdf

Kendall-Taylor, A., and Fontaine, R. (2024, April 23). *The Axis of Upheaval. How America's Adversaries Are Uniting to Overturn the Global Order*. Foreign Affairs. https://www.foreignaffairs.com/china/axis-upheaval-russia-iran-north-korea-taylor-fontaine

Keßler, C. (2024, June 27). *Between competition and co-operation: How to engage with China on climate*. Centre for European Reform. https://www.cer.eu/publications/archive/policy-brief/2024/between-competition-and-co-operation-how-engage-china-climate

Kols, R. (2018, July 3). NATO Must Meet Russia's Hybrid Warfare Challenge. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-meet-russia-s-hybrid-warfare-challenge/

Kramer, F. D. (2023, October 4). *The sixth domain: The role of the private sector in warfare*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/

Libiseller, C. (2023). 'Hybrid warfare' as an academic fashion. *Journal of Strategic Studies, 46*(4), 858-880. https://doi.org/10.1080/01402390.2023.2177987

Lopez-Rodriguez, G., Moreno-Lopez, I., Hernández-Gutiérrez, J. (2023). Cyberwarfare against Critical Infrastructures: Russia and Iran in the Gray Zone. *Applied Cybersecurity & Internet Governance*, *2*(1), 1-19. https://doi.org/10.60097/ACIG/162865

Maddison, A. (2005). *Growth and the Interaction in the World Economy: The Roots of Modernity*. AEI Press. https://www.aei.org/wp-content/uploads/2017/02/Growth-and-Interaction-in-the-World-Economy.pdf

NATO. (2020). *NATO Advisory Group on Emerging Disruptive Technologies (Annual Report, 2020)*. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf

NATO. (2021). *Strategic Foresight Analysis Regional perspectives report on Russia*. NATO HQ SACT Strategic Plans and Policy. https://www.act.nato.int/wp-content/uploads/2023/05/regional-perspectives-2021-01.pdf

NATO. (2023a, June 16). *Eighth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/230616-progress-report-nr8-EU-NATO.pdf

NATO. (2023b, August 01). *NATO Innovation Fund closes on EUR 1bn flagship fund*. https://www.nato.int/cps/en/natohq/news_217864.htm

NATO. (2023c, December 13). *NATO's new Defence Industrial Production Board meets to boost defence industrial capacity*. https://www.nato.int/cps/en/natohq/news_221435.htm

NATO. (2024a, May 2). *Statement by the North Atlantic Council on recent Russian hybrid activities*. Retrieved May 2, 2024, from https://www.nato.int/cps/en/natohq/official_texts_225230.htm

NATO. (2024b, May 07). *Countering Hybrid Threats*. https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO. (2024c, August 08). *Emerging and Disruptive Technologies*. https://www.nato.int/cps/en/natohq/topics_184303.htm

NATO. (2024d, September 5). *Resilience, civil preparedness and Article 3*. https://www.nato.int/cps/en/natohq/topics_132722.htm

NATO. (2024e, October 03). *Relations with the European Union*. https://www.nato.int/cps/en/natohq/topics_49217.htm

NATO. (2024gf, October 28). *Funding NATO*. https://www.nato.int/cps/en/natohq/topics_67655.htm

Pillai, H. (2023, April 25). *Protecting Europe's critical infrastructure from Russian hybrid threats*. Centre for European Reform. https://www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid

Polyakova, A., Lucas, E., Boulègue, M., Sendak, C., Kindsvater, S., Kuz, I., and Stone, S. (2023, November 30). *A New Vision for the Transatlantic Alliance: The Future of European Security, the United States, and the World Order after Russia's War in Ukraine*. Center for European Policy Analysis (CEPA). https://cepa.org/comprehensive-reports/a-new-vision-for-the-transatlantic-alliance-the-future-of-european-security-the-united-states-and-the-world-order-after-russias-war-in-ukraine/

Razom We Stand. (2024, June 19). *Fuelling change: Europe's battle against Russian fossil fuels*. Energy Transition. https://energytransition.org/2024/06/fuelling-change-europes-battle-against-russian-fossil-fuels/

Reinsch, W. A. and Whitney, J. (2024, June 21). *Unpacking the European Union's Provisional Tariff Hikes on Chinese Electric Vehicles*. CSIS. https://www.csis.org/analysis/unpacking-european-unions-provisional-tariff-hikes-chinese-electric-vehicles

Ruhle, M., and Roberts, C. (2021, March 19). *Enlarging NATO's toolbox to counter hybrid threats*. NATO Review. https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html

Schmidt, E. (2023, February 28). *Innovation Power. Why Technology Will Define the Future of Geopolitics*. Foreign Affairs. https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics

Schmitt, B. (2024, June 12). *Wake Up NATO: It's Sabotage*. Center for European Policy Analysis (CEPA). https://cepa.org/article/wake-up-nato-its-sabotage/

Seibt, S. (2024, May 10). *Suspected Russian sabotage: The great return of Kremlin agents to Europe?* France 24. Retrieved June 11, 2024, from https://www.france24.com/en/europe/20240510-suspected-russian-sabotage-campaigns-great-return-russian-agents-europe

Skingsley, J. (2020, December 2). *Countering Threats Below the Threshold of War*. Chatham House. Retrieved May 13, 2024, from https://www.chathamhouse.org/2020/12/countering-threats-below-threshold-war

Speranza, L., and Jens, C. (2021, February 17). Bridging the Gap: Time for an EU-NATO Strategic Dialogue on Defense Tech. Center for European Policy Analysis (CEPA). https://cepa.org/article/bridging-the-gap-time-for-an-eu-nato-strategic-dialogue-on-defense-tech/

Stoddart, K. (2024). Russia's Cyber Campaigns and the Ukraine War: From the 'Gray Zone' to the 'Red Zone'. *Applied Cybersecurity & Internet Governance*, *3*(1), 5-33. https://doi.org/10.60097/ACIG/189358

Tang, S. (2009). The Security Dilemma: A Conceptual Analysis. *Security Studies*, *18*(3), 587-623. https://doi.org/10.1080/09636410903133050

Tech Accord. (2022, May 23). *The Technology Industry and the Age of Hybrid Warfare*. https://cybertechaccord.org/the-technology-industry-and-the-age-of-hybrid-warfare/

Textor, C. (2024, April 8). China's share of rare earths production worldwide from 2016 to 2023. Statista. https://www.statista.com/statistics/1294393/share-of-global-rare-earths-production-in-china/#statisticContainer

United Nations. (2024, May 14). *Escalating Attacks on Ukraine's Civilian, Energy Infrastructure Making Humanitarian Aid Delivery Even More Dangerous, Relief Chief Tells Security Council*. Meetings Coverage and Press Releases. https://press.un.org/en/2024/sc15695.doc.htm

U.S. Department of Energy. (May 2023). *Critical Materials Assessment*. https://www.energy.gov/sites/default/files/2023-05/2023-critical-materials-assessment.pdf

Zelikow, P. (2024). Confronting Another Axis? History, Humility, and Wishful Thinking. *Texas National Security Review, 7*(3), 80-99. https://tnsr.org/2024/05/confronting-another-axis-history-humility-and-wishful-thinking/