# Emerging Tech Innovation Aff

## Notes

### Explanation

#### This is an affirmative case that proposes increased U.S. security cooperation with NATO over emerging technology innovation. The plan proposes that the U.S. strengthen NATO’s defense innovation hubs and research and development in AI, biotech, and cybersecurity. Specifically, it calls for the U.S. to increase its support of and participation in NATO’s Innovation Fund and Defense Innovation Accelerator for the North Atlantic (DIANA).

#### There are two advantages: RMA (Revolution in Military Affairs) and Alliance Fragmentation. The RMA advantage claims that the plan is necessary to maintain NATO’s military superiority over its adversaries. This is critical to prevent great power war, deter Russia, and de-escalate global hotspots.

#### The Alliance Fragmentation advantage claims that U.S. support for the NIF and DIANA is crucial to integrate the various allied defense innovation ecosystems. This is crucial to effectively counterbalance China because it unites the U.S.’s European and Asia-Pacific allies and bolsters their military capabilities.

#### This case has strong “U.S. key,” “NATO key,” and “U.S. security cooperation key” advantages. NATO is already moving ahead with its NIF and DIANA, but U.S. support has so far been only pro forma and perfunctory. The affirmative can therefore argue that the status quo links to generic “NATO Bad” and “NIF/DIANA Bad” DAs, but that the plan is crucial to solve the advantages.

### User’s Guide

#### This file includes two versions of the 1AC: an intentionally overhighlighted version and a more appropriately highlighted version. Time permitting, students should use the intentionally overhighlighted version as the basis for constructing their own version of the 1AC. During this process, students should remove redundant highlighting, improving highlighting efficiency, and revise tags to better suit their linguistic and stylistic preferences. Redundant or repetitive cards can also be removed from the 1AC for time purposes.

#### Backline materials to respond to the arguments in the negative file are organized by argument name. The “AT: CPs (General)” section includes materials that are useful against many counterplans, including the four specific counterplans in the case negative file.

#### There are significant interactions between this case and the other packet cases (about AI and cybersecurity). This affirmative could credibly claim to solve some/most of the advantages in those affirmative files, too. For the purposes of the camp tournament, your instructors will promulgate a set of rules/guidelines for what is allowed and what is not.

## 1AC (Overhighlighted)

### 1AC — RMA Advantage

#### Contention One: RMA

#### Emerging and disruptive technology (EDT) is creating a new Revolution in Military Affairs (RMA), but NATO has been slow to adapt — this will decimate its technological superiority.

Havránek and Bagge 21 — Jan Havránek, Deputy Minister of Defense of the Czech Republic, former Policy Adviser at the Policy Planning Unit at the Office of the NATO Secretary General, holds an M.A. in International Relations from Tufts University, and Daniel P. Bagge, Independent Specialist in Emerging and Disruptive Technology, former Cyber Attaché of the Czech Republic to the United States, former Director of Cyber Security Policies in the National Cyber and Information Security of the Czech Republic, former Member of the Cyber Security Strategy Expert Group at the European Union, holds an M.A. in International Relations and National Security Studies from the George C. Marshall European Center for Security Studies (Germany) and Bundeswehr University Munich (Germany), 2021 (“Technology Adoption: Are we too late to the party?,” *Small Wars Journal*, July 18th, Available Online at https://smallwarsjournal.com/jrnl/art/technology-adoption-are-we-too-late-party, Accessed 07-12-2022)

Introduction

NATO and the West are experiencing a reversed kind of revolution in military affairs (RMA) with new technologies bearing far-reaching implications beyond the conduct of war. Past revolutions in military spilled from the battlefield to the civilian sector. They had an effect either by directly impacting the result of a given conflict or through adoption of military technical advantages in non-military aspects of life. Today, we see an opposite trend brought by the private and non-military, non-governmental actors. In their everyday lives, general publics and governments alike face military-grade technologies developed and applied by the commercial sector. And it is the private sector that enjoys exclusivity over these technologies while the military lags behind.

How information is gathered, processed, analysed, communicated, distributed, and utilized has always underlined military planning and assumptions for success in conflict. For example, the reconnaissance strike complex introduced by the Soviets was based on real-time intelligence gathering and underpinned by automated systems and fast data processing. Similarly, NATO’s deep attack concept assumed that commanders “would be given the automated assessment means necessary to rapidly analyse the enemy’s force array.”[1] Such concepts, however innovative and tech-based, assumed a relatively limited amount of data and relied heavily on the human factor. Today, in the era of cloud computing and artificial intelligence, there is a clear shift towards sensor-centric, automated processing. Reconnaissance and analysis are becoming as important as firepower and kinetic effects. Humans are being pushed out from the decision-making due to the quantity of information gathered/coming from the battlefield. The hyper-speed warfare (or the “hyper war,” a term linking the intensity of conflict with cybernetics) risks making the human factor almost obsolete. To a certain extent, human presence in the loop will consequently become more a question of morality and less of efficacy.

None of this is science fiction, as modern technologies enabling hyper war already exist. The question for NATO and the West is not whether they choose to adopt these technologies but how they should adopt them to their benefit.

The situation is even more complicated if we consider the myriad of actors involved in international security. In the past, timing and accuracy of decision-making depended on a system designed by the state, was utilized on the state level, and made for the state’s purpose. Today, external entities such as corporations, non-state actors, groups of citizens and individuals matter as well. They hold the power and the technological means to exercise significant pressure over state affairs. Some even have the ability to largely cripple the functioning of governments and state services.

This development poses a significant challenge to NATO’s ability to deliver on its core tasks. If the Alliance wants to successfully continue its political-military adaptation, it will need a new approach to decision-making, operational planning, and crisis management.

This article addresses some of the key issues the Alliance needs to consider as it navigates through the new kind of revolution in military affairs: 1) the changing character of warfare; 2) the domination of the private sector over the military in the deployment of commercial technology with military potential; 3) and the interdependence of decision-making and modern technology.

The Changed Nature of Warfare

Modern technologies are changing the nature of warfare, as they have throughout the human history. In many instances, introduction of new weaponry constituted for a tactical advantage on the battlefield, occasionally reaching a strategic-level impact. An example of that can be the introduction of the British longbow at the Battle of Agincourt. Other technologies changed profoundly how militaries operate and wage war. Among such examples are railroads, telegraph, radar, combustion engine, jet engine, or radio frequencies-based communication equipment. The revolutionary nature of these technologies usually brings about significant changes in defence planning, command and control, and force organization.

For any institution, be it a nation state, a large bureaucracy, or an international alliance such as NATO, the ability to adopt disruptive technologies is key. The adoption usually leads to a larger structural adaptation: The use of standardized calibres in the French Revolutionary and Napoleonic Wars allowed for greater flexibility and uniformity of the French forces. The first use of Marconi’s wireless telegraphy by the British armed forces in the Anglo-Boer War (1899-1902) changed the way how military communicated. The use of railroads in the 19th century wars had a strategic effect on the mobility and supply of forces. Finally, the deployment of radar technology during World War 2 improved both defensive and offensive capacities of the militaries, and, as a result, probably saved thousands of lives. In all these instances, the military advancement of technologies spilled over to the civilian side as well.

In the past five decades, military science theorists have been dealing with the evolution in warfare in more detail. Although the main focus was dedicated to the then-ongoing Cold War, scholars from the field made a number of predictions that have proven to be correct. They correctly understood that technological advancement was gaining momentum and that the upcoming changes were not going be evolutionary but would come in leaps.[2]

Three concepts also emerged from this thinking: military technical revolution (MTR), revolution in military affairs (RMA), and military revolution (MR). Even though they stand individually, all three concepts are closely interconnected. For example, technology or a weapon platform that has reached the level of military technical revolution can, in the end, reach the level of military revolution as long as it constitutes considerable changes to organizational structure and operational art. In several cases, the MTR, RMA and MR are seen as one concept altogether.[3]

Military Technical Revolution, Revolution in Military Affairs, and Military Revolution

An event has to meet several conditions to qualify as a MTR/RMA/MR. A revolution is defined by a profound change in military systems, operational art, and organizational adjustment. Simple introduction of new technology or military platform does not constitute an MTR.

As Andrew F. Krepinevich, a defence policy analyst, writes,[4] a real-world example of military technical revolution can be unmanned combat vehicles and their role in conducting combat and ISR operations. Another example are cyber defence/offense oriented forces that fulfil the following criteria: technological change—introduction of new military platforms; evolution of military systems; operational innovation (e.g., cyberspace defence planning); or organizational adaptation impacting force structure and organizational units.

A military revolution in effect alters the way in which power is projected. Apart from changing the shape and form of warfare, it spills over from the military organizational structures and battlefields into societal, economic, and political domains.

The above-mentioned enablers of military revolution, such as artificial intelligence and quantum technology applications, show promising potential in changing the current societal fabric and effectively impacting societal, political, and military affairs.

Among the decisive factors, universal to all combat operations, is time. As the pace of technological advancement increases, the potential effects of a technology are no longer the most important factor. Equally important is the pace of adaption: how fast a technology can be utilized and how it recalibrates the relation between action and reaction. As time remains of immense importance, the ability to share information and move forces around based on that information can be the decisive factor in conflict. The speed of information sharing can thus be considered a military revolution.[5] The introduction of combustion engines and the changes it brought to operational art, manoeuvring, and transport of forces, changed the time factor. Unparalleled sensory awareness, communication, and automation have the same potential.

Consequently, time available for decision-making will continue to shrink. Decision makers will have to be equipped with information and intelligence as accurate as possible. The “speed of information” will be critical to provide political guidance to commanders or even to conduct a pre-emptive strike. There may be instances when the pace of combat operations will increase to a threshold where defensive action will be rendered useless.[6] Technology that can process this “speed of information” will affect the entire decision-making algorithm and broader perception of security and defence in society.

Militarization of Technology and the Role of Private Sector

The 21st century introduced an unparalleled speed of innovation and dissemination of (digital) technology among the general population and the private sector. It also hindered states’ ability to remain the sole proprietor of military grade applications. This is due to an unprecedented redistribution of applied research from the government level towards the private sector. Today, private entities commercialize disruptive technologies and provide them directly to the customers, unleashing military level applications into the wild. The governments, namely national security and defence domains are lagging behind in adoption of innovative technologies. This is evident from the spending on military research and development, which is dim in comparison to its private sector equivalents.[7] For example, in 2004, the global spending on civilian research and development was approximately ten times as large as global military research and development.[8]

Emerging disruptive technologies are thus becoming more accessible. The interdependency between state instruments of power (including armed forces) and civilian technology is growing and is expected to grow even further. In the past, military platforms were developed by the private sector, but their sole purpose was defined by the military. Today’s world brings the challenge of dual-use technology that is researched, manufactured, and provided entirely by the private sector, while having military application. Which effectively impacts the competitiveness on the battlefield. With facial recognition, targeting, and other artificial intelligence-powered applications (including micro targeting on social networks), the interest of the private sector and state actors overlap and are often blurred. It is common for state actors to be dependent on private sector providers. Sometimes to the extent where the government is unable to adjust the technologies’ conditions for its purposes, as the usual customer base lies in the civilian business world.

The rise of corporations and digital tycoons brought about democratization of technologies and their global spread in an unprecedented speed, resulting in a digital interdependency. States have been replaced by private entities who hold the keys to information flow and disruptive technologies. These technologies are often introduced to the general public sooner than the governmental bodies even have a chance to understand them.

Technological superiority has always played a significant role in international relations. It usually derived from the use of force and was traditionally in the hands of the state. In the past few decades, non-state entities started surpassing the state’s control. Technology provided by corporations paired with ideology and strategic interests of various state actors. However, state actors were not equipped with proper organizational structures and decision-making processes to stay up to date. As result, they have been left behind not to lead, but to react to technological progress and innovations.

Quantum research on sensors[9] can be an example of the private sector’s success. Non-state actors currently both employ the leading scientists in the field and conduct research in cooperation with competing state interests. All that despite the efforts of the governmental bodies and the military to fund innovative research.[10] This substantially increases the prospects of quantum related applications being provided to the general population before they are utilized by the military, leading to a loss in competitiveness on the battlefield.

The issue is caused by the inability of governmental entities to appreciate the need to conduct basic and applied research competitively with the private sector. In order for it to be done correctly, it would require a substantial organizational change and the ability to understand the potential impacts of disruptive technologies. That is also necessary for proper resource allocation. Modern and disruptive technologies are part of the non-conventional military risks and destabilizing efforts that governmental structures fail to address. A number of technological platforms, social networks, and digital enablers have become tools of digital deceit. They have been used to target the general population, which was unaware of being exposed to hybrid tactics and military grade influence operations.[11] This was enabled by overlaps of influence-operation techniques from the military field into the private sector. Private companies also applied these techniques in target group advertising.

This is not the first time the West has had to deal with ideological competitors trying to gain supremacy. The Cold War was about both ideology and technology, with the stark example of Operation Farewell.[12] Even then, technological superiority was meant to promote ideological and strategic interests. The combination of ideology and technology continued to be a factor in the post-Cold War world. An example of that can be terrorist organizations and their use of basic available technology. The situation in 2021 is, however, starkly different from the 1980’s or the 2000s for a number of reasons:

\* As argued earlier, the character of warfare has changed profoundly; technologically driven warfare has entered the soft power arena.

\* The pace of military operations and general interactions has increased— he human capacity is now limited not only by the speed of events but also by the amount of information collected, processed, and analysed from the battlefield. The ISR platforms are collecting so much data and raw intelligence that it is necessary to automate processes previously not constrained by human capacity or reaction speed demands. The changes pushing the limits of human operators and analysts happen in leaps and are fast paced.

\* What is more: private sector capacities play a significant role in international power competition. Technological tycoons represent stand-alone actors risen on the wealth and influence of the technology they provide. They have also become the tools of state influence. Understanding this shift is hard, as we tend to differentiate between private entities, corporations with presence on the global markets, and state actors. However, in many cases, the private corporations are bound by national legislation, hiding as agents of influence in plain sight.

\* As a result, we see traditional technological powers (the West, led by the United States, with Europe lagging behind) and democratic tech tycoons, including Japan, South Korea, and Taiwan, capitalizing on the asymmetry provided by modern technologies. While China, Russia, and India aspire to supersede them, this aspiration is evident from both their official policies and their investment in new technologies and defence modernization. What started as mainly intellectual property transfer and theft[13] has now turned into a full-fledged technological adoption race.[14]

Implications for NATO

So where does all this leave NATO? In 2021, as NATO has already begun to define its vision for the next ten years, it faces three principle challenges:

1. Ensuring that decision-makers understand the sheer potential derived from emerging and disruptive technologies and how they will impact the Alliance’s governance and decision models.

2. Prioritizing what technologies, the Alliance should pursue, when, and how they fit into NATO’s wider posture;

3. Sharing the technological burden equally across the Alliance.

Raising awareness among political leaders about the new technologies’ impact on NATO may not be as simple as it seems. Currently, there is a growing gap in perception of the new technology’s importance between the political and military level. Military authorities of the Alliance have, for a long time, been highlighting the need for innovation and adoption of new technologies.[15] Trials of innovative technological solutions and new capabilities have been part of NATO’s military training and exercises. For example, NATO now regularly tests unmanned systems in the maritime area[16] and there is work being done in the area of Electronic Spectrum warfare. Furthermore, adoption of new technologies in new capabilities development has been encouraged through the NATO Defence Planning Process (NDPP). In 2018, the Allied Command Transformation developed Emerging and Disruptive Technologies Roadmap, which received political endorsement at the meeting of defence ministers in June 2019.

On the political front, the effort has been slower. Until recently, the Allies themselves have maintained a rather declaratory approach to technology and innovation. Later, in 2020, the Secretary General appointed an innovation advisory group to provide counsel on NATO’s next steps in the tech area. A full political strategy on the emerging and disruptive technologies was finally adopted at the Brussels Summit in June 2021: “[T]his strategy seeks to preserve our interoperability; safeguard our sensitive technologies; and actively address the threats and challenges posed by technological developments by others, both now and in the future. Drawing on the extensive innovation expertise of all 30 Allies, we will further leverage our partnerships, including with the private sector and academia, to maintain our technological edge.[17]”

The Allies pledged to launch a civil-military Defence Innovation Accelerator for the North Atlantic (DIANA) and to establish a NATO Innovation Fund. The aim is to promote interoperability, foster development and adoption of technological solutions, and to allow individual NATO Members to support start-ups working on dual use emerging and disruptive technologies relevant to NATO’s security. The Allies also agreed to continue developing capabilities in the technological domain and recognized the need for research and development and innovation to meet the challenges emerging and disruptive technologies pose. Some of the specific areas where new capabilities must be acquired are air-to-air refuelling, training, precision strike, munitions, air defence, CBRN defence, autonomous systems, and next-generation rotorcraft capability.[18]

The process will require effective prioritization. The afore-mentioned NATO Defence Planning Process already accounts for future technological change in military capability development. Allies have a free reign in how they wish to meet the target, including what platform and technology they wish to choose. The pitfall of this approach lies in the traditional view of military technology adoption and capability development. More specifically, the issue is the government-centric model that operates with significantly longer lifecycles as well as the ownership structures that find no applicable parallel in the private sector’s current pacing and push out of emerging and disruptive technologies.

It will be up to NATO to use both its new and already-existing tools to help navigate through these technologies and decide on which to adopt first. Together with the Allies and the private sector, NATO/DIANA should scan the horizon and say which new technologies are to be integrated with highest priority. NATO must then proceed with the integration into its planning (both capability and civil emergency), training and exercises, as well as the Alliance’s wider consultation and decision-making.

The adoption must happen systematically, at the highest political level. The Brussels Summit should be an impulse for the Council to start incorporating more technologically driven discussions into its deliberations. Scenario-based discussions and NATO’s high-level exercise program should include situations where emerging and disruptive technologies play a decisive role. None of this requires any radical changes to the decision-making procedures or new tools.

Although the NATO Innovation Fund is a step in the right direction, it must reflect the disparities that exist among individual Member States in this context. Many Allies have national assets that fulfil various tech innovation functions. For example, the UK’s jHub Defence Innovation helps integrate market-ready solutions into military.[19] In 2020, Germany established an agency for innovation in cyber security to promote technological innovation and solutions that would enhance the country’s security.[20] NATO should serve as a platform where nations with more advanced structures, know-how and capabilities come forward and share some of these solutions and findings with other Allies.

The NATO Innovation Fund should also facilitate burden-sharing in this area. Emerging and disruptive technologies have so far been guarded as a national treasure; their application and availability in multinational context has been scarce. In the future, not all Allies will possess or have access to new technologies shaping the military capabilities and conduct. Some countries will be faster in technological adoption. Others may not be able to afford new technologies, if they are to meet all other requirements for NATO’s collective defence. The Fund can be a mechanism that balances out these gaps and spreads the burden more equally among the Allies. NATO must now design a system of allocation—currently envisioned on a voluntary basis—that will motivate the Allies to contribute to it. This must take into account national requirements that might be limiting for some Allies and the danger of duplicity with similar endeavours.

There are several examples of sharing mechanisms that NATO has successfully adopted in the past and can now build on: 1) Nuclear-sharing arrangements where non-nuclear members of NATO support potential nuclear missions and the decision-making without possessing the nuclear technology; 2) Common-funded capability models, such as the Allied Ground Surveillance system or NATO’s Ballistic Missile Defence, where Allies fund and outsource the development of technology through common / joint financial contributions; while both slightly different in structure and funding, both are an example of technology funded by some Allies, but made available to the entire Alliance. Both examples link to previous revolutions in military affairs. Until now, the closest the Allies have come to having a new technology sharing mechanism is the Sovereign Cyber Effects Provided Voluntarily by Allies mechanism. It allows the Supreme Allied Commander Europe (SACEUR) to request offensive effects to be delivered on a designated target, without sharing the technology with others.[21]

All these examples have one thing in common: technological know-how and intellectual property remains in the hands of the capability providers. This gives NATO an opportunity to forge new tech-sharing arrangements that would include individual Allies and the private sector. This could also prevent the technological gap among Allies from widening any further.

One specific solution could be creating a private sector parallel to NATO’s political partnerships. However, the criteria for such partnerships might be hard to agree on. NATO would have to find a way to satisfy some highly political questions, such as: What companies and what technologies would be represented? Or would Allies even be able and willing to generate funds to support a NATO-branded research & development?

In the meantime, NATO must approach the prioritization of emerging and disruptive technologies by employing its traditional strengths: define its technological requirements through the prism of military requirements and forge a consensus among thirty Allies on the general technological pathway. When NATO sets the standards, individual Allies are usually very capable of delivering, according to their national preferences and legislation.

Lastly, in its ongoing efforts to address the challenge of emerging and disruptive technologies, NATO must take into account similar, already existing or maturing projects and structures. The European Union sees emerging and disruptive technologies as a crucial issue and has developed mechanisms through which they are tackled. The European Defence Agency recognizes technological development as one of the main pillars of its work and provides a useful platform for international cooperation. It aims to support Member States in developing and improving capabilities on a cutting-edge technological level of its Member States and shape their national strategies in this area. The European Defence Fund deals with both technological research and defence capability development and even specifically allocates a part of its financial resources for disruptive technologies.

A major task for the two organizations will now be to find a way to cooperate on this issue and avoid undesirable duplication. The Alliance and the EU must come up with a solution where the EuroAtlantic area is capable of adapting to the ever-changing security environment and can readily adopt fast-advancing technologies. What is more, both sides of the Atlantic must be equally capable partners in this cooperation and burden sharing.

Conclusion

Technological change is real, fast paced, and greatly affects NATO’s civilian-military structures. Never has the Alliance faced so many technological changes that would reach beyond the traditional realm of security and defence.

In the 1990s, the key political question for the future of NATO was whether to adapt by going out of area (in terms of operations and membership) or go out of business. The question for the next couple of years is essentially the same; it touches the very purpose and existence of the Alliance and the utility of NATO: How to make sure that NATO stays technologically relevant so that it can maintain its function and capabilities. Complacency and general political statements will not suffice. The private sector, which is the principal agent of the new kind of revolution in military affairs, is technologically advancing in leaps. If NATO is not able to keep up with this change in organization of geopolitics and technology, it will have to change its organizational structure. With modern and disruptive technologies becoming more mainstream and moving into wider governance structures, similar adjustments will be necessary in NATO’s daily business operations.

NATO can successfully navigate the new wave of revolution in military affairs; however, it must first change its political culture and overall approach to modern and disruptive technologies. It also needs to develop new technology-sharing mechanisms that will be fair to all Allies. There may be different approaches to this change: a reform of NATO’s procurement agencies, a reform of financial mechanisms, or a partnership reform. Either way, any such effort will have to build on the active participation of the private sector. Only then will NATO be able to maintain its technological edge in the future.

#### Failing to maintain NATO’s technological superiority will cause great power nuclear war — out-competing Russia and China in the EDT RMA is key.

Kroenig 21 — Matthew Kroenig, Professor in the Department of Government and the Edmund A. Walsh School of Foreign Service at Georgetown University, Director of the Global Strategy Initiative and Deputy Director of the Scowcroft Center for Strategy and Security at the Atlantic Council, former Special Government Employee and Senior Policy Adviser to the Office of the Assistant Secretary of Defense for Strategy, Plans, and Capability/Nuclear and Missile Defense Policy at the U.S. Department of Defense, former Stanton Nuclear Security Fellow at the Council on Foreign Relations, holds a Ph.D. in Political Science from the University of California-Berkeley, 2021 (“Will Emerging Technology Cause Nuclear War?: Bringing Geopolitics Back In,” *Strategic Studies Quarterly*, Volume 15, Issue 4, Winter, Available Online to Subscribing Institutions via EBSCO Open Access Journals, p. 64-70)

***[\*\*\* Note: 4IR*** *= “The world is experiencing a fourth industrial revolution (4IR) in which a wave of new and transformative technologies is being developed, including artificial intelligence (AI), additive manufacturing, quantum information technology, hypersonic missiles, biotechnology, and directed energy.4 While these technologies are expected to have profound implications for societies and economies, most are dual use and will also affect national security, including nuclear strategic stability.” (p. 59)* ***\*\*\*]***

New Tech Arms Race

Many analysts believe the emerging technology of the 4IR could profoundly affect military capabilities and operational concepts.35 New technology has had revolutionary effects on warfare and international politics throughout history from the Bronze Age to the gunpowder and nuclear revolutions.36

New technologies with direct military application are in development, including AI, quantum information technology, hypersonic missiles, directed energy, additive manufacturing, and biotechnology. How exactly these technologies will affect the future of warfare is still uncertain. The [end page 64] National Defense Strategy Commission report charges that the United States lacks clear operational concepts for combat with Russia and China.37 Still, there is reason to believe these new technologies could have meaningful military applications but perhaps not to the advantage of the United States and its Allies and partners. At present, Russia and especially China might transcend the United States and its Allies and partners in some key 4IR technologies.

Indeed, AI could transform the future of warfare, including through the development of lethal autonomous systems.38 These “killer robots” may lower the threshold of conflict by allowing political leaders to take a country to war without risking the lives of human soldiers. When produced in large numbers, these drones could operate in swarms that overwhelm enemy military platforms and targets.39

Artificial intelligence could also be employed to rapidly sort through vast quantities of data, improving intelligence, surveillance, and reconnaissance and making it easier to track and target enemy forces. The United States retains important advantages in AI, including through its world-leading university system. But China, with its large population and surveillance tactics, has access to more data to train its AI algorithms.40 Beijing is also less constrained by ethical and moral concerns and has the lead in some applications of AI, including facial-recognition technology.

Quantum computing promises information advantages including the ability to have secure, encrypted communications and to decode enemy communications. In its 2021 Military Balance report, the International Institute for Strategic Studies states, “the integration of quantum technologies currently represents one of the most anticipated advances for armed forces. … There is little doubt that they will have disruptive effect when they are employed at scale.”41 China may have the edge in this area, as it was the first country to conduct a successful test of a quantum satellite.42

Space and cyber are increasingly important military domains. Space-based weapons, sensors, defensive interceptors, and the diffusion of counterspace capabilities will make space an increasingly contested military environment.43 The United States is relatively more dependent on space-based assets and computers than its rivals, and the US Department of Defense warns Russia and China will likely employ cyber and counter- space attacks in the early stage of any conflict with the United States in a bid to disrupt US command, control, communications, computers, intel- ligence, surveillance, and reconnaissance (C4ISR).44

Hypersonic missiles, maneuverable and able to travel at over five times the speed of sound, could allow states to conduct low- or no-warning attacks [end page 65] and to evade missile defenses.45 These weapons could also execute large-scale, nonnuclear strategic attacks, the rate of speed compressing the decision-making time leaders have to respond to such attacks. Although the United States developed the initial concepts for these weapons, Russia and China have prioritized their production, testing, and deployment. China has conducted more hypersonic tests than any other nation, and Moscow and Beijing have deployed hypersonic weapons.46

Many other emerging technologies have military applications. Directed-energy microwaves and lasers could allow states to develop more effective integrated air and missile defense systems or to degrade an enemy’s command and control.47 Additive manufacturing could greatly reduce the cost of producing component parts of military platforms and creates the potential for large and rapid quantitative increases in weapons systems, from drones and tanks to submarines and nuclear weapons.48

Biotechnology could be exploited to produce “super soldiers.” China has genetically engineered beagles with three times the muscle mass of a typical canine, a technology that could possibly be applied to humans.49 Exoskeletons could provide soldiers with superhuman strength, and brain implants promise superior cognitive performance. China employed exoskeletons in combat in its 2020 border conflict with India.50

It is not yet clear how these new technologies, when combined with novel operational concepts, will affect the future of warfare, but it is likely they will. A future state may, for example, be able to use additive manufacturing to produce masses of inexpensive drones directed by new AI algorithms to swarm and overwhelm adversaries.51 The attack might be preceded by cyber and counterspace attacks that blind an adversary and disrupt its command and control.

Following a successful advance, the country could then employ directed-energy weapons, autonomous mines, and other advanced defenses to lock in territorial gains and thwart enemy attempts to roll back its aggression. It is possible that the first state to hone these technologies and devise effective operational concepts will have a military edge over its opponents.

Novel Applications

How will states use such a newfound advantage? Technology rarely fundamentally changes the nature or objectives of states. More often, states use technology to advance preexisting geopolitical aims. Moreover, enhanced power can result in greater ambition. Given the geopolitical landscape described, it is likely the United States and its Allies and partners at the core [end page 66] of the international system will behave differently with new military technologies than will revisionist powers, such as Russia and China.

The spread of new technology to the United States and its Allies and partners would likely serve, on balance, to reinforce the existing sources of stability in the prevailing international system. At the end of the Cold War, the United States and its Allies and partners achieved a technological- military advantage over its great power rivals, with the US using its unipolar position to deepen and expand a rules-based system. They also employed their military dominance to counter perceived threats from rogue states and terrorist networks. The United States, its Allies, and partners did not, however, engage in military aggression against great power, nuclear-armed rivals or their allies.

In the future, these status quo powers are apt to use military advantages to reinforce their position in the international system and to deter attacks against Allies and partners in Europe and the Indo-Pacific. These states might also employ military power to deal with threats posed by terrorist networks or by regional revisionist powers such as Iran and North Korea. But it is extremely difficult to imagine scenarios in which Washington or its Allies or partners would use newfound military advantages provided by emerging technology to conduct an armed attack against Russia or China.

Similarly, Moscow and Beijing would likely use any newfound military strength to advance their preexisting geopolitical aims. Given their very different positions in the international system, however, these states are likely to employ new military technologies in ways that are destabilizing. These states have made clear their dissatisfaction with the existing international system and their desire to revise it. Both countries have ongoing border disputes with multiple neighboring countries.

If Moscow developed new military technologies and operational concepts that shifted the balance of power in its favor, it would likely use this advantage to pursue revisionist aims. If Moscow acquired a newfound ability to more easily invade and occupy territory in Eastern Europe, for example (or if Putin believed Russia had such a capability), it is more likely Russia would be tempted to engage in aggression.

Likewise, if China acquired an enhanced ability through new technology to invade and occupy Taiwan or contested islands in the East or South China Seas, Beijing’s leaders might also find this opportunity tempting. If new technology enhances either power’s anti-access, area-denial network, then its leaders may be more confident in their ability to achieve a fait accompli attack against a neighbor and then block a US-led liberation. [end page 67]

These are precisely the types of shifts in the balance of power that can lead to war. As mentioned previously, the predominant scholarly theory on the causes of war—the bargaining model—maintains that imperfect information on the balance of power and the balance of resolve and credible commitment problems result in international conflict.52 New technology can exacerbate these causal mechanisms by increasing uncertainty about, or causing rapid shifts in, the balance of power. Indeed as noted above, new military technology and the development of new operational concepts have shifted the balance of power and resulted in military conflict throughout history.

Some may argue emerging military technology is more likely to result in a new tech arms race than in conflict. This is possible. But Moscow and Beijing may come to believe (correctly or not) that new technology provides them a usable military advantage over the United States and its Allies and partners. In so doing, they may underestimate Washington.

If Moscow or Beijing attacked a vulnerable US Ally or partner in their near abroad, therefore, there would be a risk of major war with the potential for nuclear escalation. The United States has formal treaty commitments with several frontline states as well as an ambiguous defense obligation to Taiwan. If Russia or China were to attack these states, it is likely, or at least possible, that the United States would come to the defense of the victims. While many question the wisdom or credibility of America’s global commitments, it would be difficult for the United States to simply back down. Abandoning a treaty ally could cause fears that America’s global commitments would unravel. Any US president, therefore, would feel great pressure to come to an Ally’s defense and expel Russian or Chinese forces.

Once the United States and Russia or China are at war, there would be a risk of nuclear escalation. As noted previously, experts assess the greatest risk of nuclear war today does not come from a bolt-out-of-the-blue strike but from nuclear escalation in a regional, conventional conflict.53 Russian leaders may believe it is in their interest to use nuclear weapons early in a conflict with the United States and NATO.54 Russia possesses a large and diverse arsenal, including thousands of nonstrategic nuclear weapons, to support this nuclear strategy.

In the 2018 Nuclear Posture Review, Washington indicates it could retaliate against any Russian nuclear “de-escalation” strikes with limited nuclear strikes of its own using low-yield nuclear weapons.55 The purpose of US strategy is to deter Russian strikes. If deterrence fails, however, there is a clear pathway to nuclear war between the United States and Russia. [end page 68] As Henry Kissinger pointed out decades ago, there is no guarantee that, once begun, a limited nuclear war stays limited.56

There are similar risks of nuclear escalation in the event of a US-China conflict. China has traditionally possessed a relaxed nuclear posture with a small “lean and effective” deterrent and a formal “no first use” policy. But China is relying more on its strategic forces. It is projected to double—if not triple or quadruple—the size of its nuclear arsenal in the coming decade.57

Chinese experts have acknowledged there is a narrow range of contingencies in which China might use nuclear weapons first.58 As in the case of Russia, the US Nuclear Posture Review recognizes the possibility of limited Chinese nuclear attacks and also holds out the potential of a limited US reprisal with low-yield nuclear weapons as a deterrent.59 If the nuclear threshold is breached in a conflict between the United States and China, the risk of nuclear exchange is real.

In short, if a coming revolution in military affairs provides a real or perceived battlefield advantage for Russia or China, such a development raises the likelihood of armed aggression against US regional allies, major power war, and an increased risk of nuclear escalation.

Implications

Future scholarship should incorporate geopolitical conditions and the related foreign policy goals of the states in question when theorizing the effects of technology on international politics. Often scholars attempt to conceptualize the effects of weapons systems in isolation from the political context in which they are embedded.

Studies treat technology as disembodied from geopolitics and as exerting independent effects on the international system. But technology does not float freely. Technology is a tool different actors can use in different ways. Bakers and arsonists employ fire in their crafts to strikingly different ends. In the current international environment, Russia and China would tend to employ technology toward advancing revisionist aims. Technological advances in these countries are therefore much more likely to disrupt the prevailing international order and nuclear strategic stability.

This approach also suggests the potential threat new technology poses to nuclear strategic stability is more pervasive than previously understood. To undermine strategic stability, new technology need not directly impact strategic capabilities. Rather, any technology that promises to shift the local balance of power in Eastern Europe or the Indo-Pacific has the potential to threaten nuclear strategic stability. [end page 69]

This understanding of this issue leads to different policy prescriptions. If the technology itself is the problem, then it must be controlled and should not be allowed to spread to any states. In contrast, the framework outlined here suggests a different recommendation: preserve the prevailing balance of power in Europe and Asia. Technological change that, on balance, reinforces the prevailing international system should strengthen stability.

Leading democracies, therefore, should increase investments in emerging technology to maintain a technological edge over their adversaries. Export control and nonproliferation measures should be designed to deny emerging military technology to Russia and China. Arms control should be negotiated with the primary objective of sustaining the current international distribution of power. Making progress in these areas will be difficult. But the consequences of failure could be shifts in the international balance of power, conflict among great powers, and an increased risk of nuclear war.

#### NATO EDT superiority will cement effective deterrence — quickly getting innovative tech to the battlefield is key.

Hodges 21 — Ben Hodges, Pershing Chair in Strategic Studies at the Center for European Policy Analysis, Retired Lieutenant General in the U.S. Army where he served as Commanding General of the United States Army Europe, Senior Associate Fellow at the Royal United Services Institute for Defense and Security Studies (UK), 2021 (“Defense Technologies… for What? Speed, Speed, Speed!,” Center for European Policy Analysis, February 17th, Available Online at https://cepa.org/defense-technologies-for-what-speed-speed-speed/, Accessed 07-10-2022)

Giving our armed forces the proper technologies to perform their mission will ultimately ensure that deterrence never fails.

The key to effective deterrence for the transatlantic alliance is speed: speed of recognition of the Kremlin’s malign activities; speed of decision to start necessary deployments, movements and related activities; and speed of assembly to move faster than the Kremlin to pre-empt attacks and signal our preparedness to act. Fortunately, a wide range of new technologies are emerging and evolving that can improve speed, if they are properly integrated into our armed forces and into our plans.

New technologies that have the greatest potential to this end include artificial intelligence, machine learning, automated systems, hypersonics, and cyber technologies, among others. All these tools can enhance decision-making, improve interoperability of mission command systems and logistics, help counter adversaries’ unmanned air and maritime systems, and facilitate material changes to improve military mobility. Key to maximizing the impact of these new technologies, and to making the investment worthwhile, is coordination among political decision-makers and industry innovators to understand Allies’ needs and meet capability requirements.

Below are some examples of those needs and corresponding technological requirements. Though in need of refinement, these provide an azimuth for innovators, policymakers and industry leaders across the transatlantic community to improve our collective speed and enhance effective deterrence.

Need for Speed of Recognition: Recognizing threats, indicators, and warnings from our adversaries has become increasingly difficult within the context of hybrid warfare. Unlike in the Cold War, when the first indicator of an attack may have been T72 tanks coming over the horizon, today, the first indicator may be a cyber-attack that shuts down transportation or financial systems. It could be a dockworkers’ strike in a Baltic port, or even attacks on transportation infrastructure by hypersonic missiles. Being able to see these possibilities as they are taking shape, before they are effective, is necessary to prevent or respond to an emerging crisis.

Requirement: Technologies that can fuse the wide range and variety of intelligence and information as part of NATO’s indicators and warnings network are vital. A U.S. satellite will most likely not be the first system to detect a hybrid threat or activity. Instead, it could be a human source, perhaps a customs agent, border guard, or member of a territorial force. But how does information about a dockworkers’ strike in a Baltic port turn into analysis, for instance, that reveals this strike was created artificially by FSB operatives to create a pretext for the Kremlin to interfere abroad? The key lies in the ability to quickly and accurately parse through all available data and reports — across national and interagency boundaries, NATO and non-NATO nations, five-eye and non-five-eye nations — using artificial intelligence, machine learning, and other fusion capabilities. This also requires protecting information networks from hacks, malware, and other attacks, all the while facilitating the sharing of sensitive and classified information, using sophisticated cyber defenses.

Need for Speed of Decision: Authorizing movements and actions to prevent or respond to an emerging crisis, within a NATO context, requires the unanimous consent of all 30 member states. Decisions to start moving capabilities, pull ammunition such as Patriot “Interceptors” out of storage depots, and reprioritize military movements, demand high-level decision-makers to act quickly and decisively, despite the sensitive nature of these activities. The Kremlin is fully aware of NATO’s decision-making process, the requirement for unanimous consent, and the political reluctance to delegate such decisions about movement to operational commanders, and they aim to exploit that gap through their own centralized decision-making.

Requirement: This means Allied and partner political decision-makers need to have access to a variety of information, plans, options, and shared courses of action to create appropriate signals and communicate tasks to commanders in a timely manner. That’s why it’s critical to leverage technologies such as synthetic environments and human augmentation, which can enable Allied political leaders to simulate complex, multi-domain environments, test time-sensitive decision-making, and physiological responses, and course-correct in advance through sustained exercises and training.

Need for Speed of Assembly: NATO must demonstrate that allies are able to move as fast, or faster than, Russian Federation forces to prevent or react to an emerging crisis. The key is signaling to the Kremlin that any malign activities will either fail or be too costly to attempt. Still, NATO must do this in such a way that it does not unnecessarily provoke or escalate tensions with Russia. This requires assembling key forces and capabilities quickly and strategically in pre-crisis or peacetime conditions.

Requirement: In order to assemble fast enough, technologies are needed to protect against cyber-attacks against transportation and power-generation infrastructure and reduce the weight and size of modern armored vehicles which are difficult to move quickly across the continent to the frontline. Using technology to develop affordable bridging assets necessary for the many river crossings in Europe, as well as to protect against Russian unmanned systems and create a NATO anti-access aerial denial (A2AD) bubble, should be priorities. Automated systems — from robots and drones to active cyber defense as well as new missile technologies — can play crucial roles in protecting allied and partner deployments and critical infrastructure.

At the end of the day, deterrence depends on the women and men of our armed forces being trained and ready. Giving them the proper technologies to perform their mission will give them the advantages needed to improve awareness, preparedness, and speed and, ultimately, ensure that deterrence never fails.

#### NATO deterrence prevents global hotspot escalation and great power war.

Dowd 22 — Alan W. Dowd, Senior Fellow in the Center for America's Purpose at the Sagamore Institute—a think tank, Senior Fellow at the Fraser Institute and the American Security Council Foundation, Contributing Editor and Columnist at the American Legion Magazine, former Adjunct Professor of American Foreign Policy at Butler University and Anderson University, 2022 (“Putin’s war, NATO’s unity, Ukraine’s valor,” *American Legion Magazine*, March 15th, Available Online at https://www.legion.org/landingzone/255256/putin%E2%80%99s-war-nato%E2%80%99s-unity-ukraine%E2%80%99s-valor, Accessed 04-04-2022)

**[\*\*\* Note: 9/11 refers to the September 11, 2001 terrorist attacks against the United States; 11/9 refers to the November 9, 1989 fall of the Berlin Wall.]**

Vladimir Putin’s “unprovoked, unjustified, unconscionable war” has taken thousands of lives, destroyed much of Ukraine’s modern infrastructure and ancient landmarks, and created the largest tidal wave of refugees in Europe since World War II. Yet amidst all these horrors, there’s a flicker of hope: The NATO alliance is more united than at any time since 9/11 – and more important than at any time since 11/9. This is the very opposite of what Putin expected.

Common cause

Consider how the 30-member alliance swiftly rejected Putin’s December demands that NATO not expand to include Ukraine, cease its deterrence operations in Eastern Europe and grant him veto authority over the decisions of sovereign nations. Then, as Putin massed more than 180,000 troops, hundreds of tanks and dozens of warships on Ukraine’s borders and coasts, the alliance set about the task of bolstering its easternmost members.

The United States deployed B-52s to Britain; F-35s to Germany, Lithuania and Estonia; F-15s to Poland and Estonia; F-16s to Romania; dozens of AH-64 attack helicopters to the Baltics and Poland; Patriot air-defense batteries and thousands of combat troops to Poland; an armored brigade combat team of 7,000 soldiers to Germany; hundreds of troops to Hungary, Bulgaria and Romania; and 800 combat troops to the Baltics. There are now about 100,000 U.S. troops standing guard all across Europe.

In addition, Washington approved a long-delayed sale of 250 M1A2 tanks to Poland, and surged the aircraft carrier USS Harry S. Truman to join carrier strike groups from Italy and France in a show of force in the northern Mediterranean.

Britain has deployed hundreds of troops to Poland, sent warships to the Black Sea and eastern Mediterranean, dispatched Challenger tanks to the Baltics, doubled its troop commitment in Estonia, and based fighter-bombers in Romania and Poland. Canada has deployed hundreds of additional troops to augment its battlegroup in Latvia. Germany has sent troops to reinforce its contingent in Lithuania. France has deployed hundreds of troops to Romania. Germany and the Netherlands sent Patriot batteries to Slovakia. Denmark rushed F-16s to Lithuania and sent a frigate to the Baltic Sea. Dutch F-35s and Spanish Eurofighters deployed to Bulgaria. NATO now has 130 warplanes on “high alert” in Central and Eastern Europe, more than 200 ships forward-deployed in the waters of the Arctic, North Atlantic, Baltic, Aegean, Adriatic and Mediterranean, and tens of thousands of newly deployed or repositioned combat troops in the region, according to NATO Secretary General Jens Stoltenberg.

For the first time in history, NATO activated and deployed its rapid-response force. And for just the second time in history, Turkey – acting under international authorities it was granted by a 1936 treaty – closed the Black Sea to Russian warships.

NATO hasn’t limited its response within its footprint. In a ~~crippling~~ [crushing] blow to Russia’s economy, NATO members, the EU, Japan and other partners disconnected Russian banks from SWIFT, the global messaging system that enables financial transfers among 11,000 banks in 200 countries. Britain, Canada and the European Union joined the United States and other partners in imposing “unprecedented export control measures” to cut off Russia’s access to high-tech products. The allies closed their airspace to commercial and private Russian aircraft, seized Russian assets, and cut off Putin’s kleptocracy from the most of the world.

Specific to Ukraine, before the invasion, the United States flew reconnaissance flights over eastern and western Ukraine, shared intelligence with Kiev, and formed an airbridge linking NATO bases with Ukraine. This enabled delivery of defensive weapons from North America, Britain and Europe.

When Russia started to fill Ukraine’s skies with missiles and artillery, NATO began delivering weapons overland. In the first six days of the war, the alliance rushed 17,000 antitank weapons into Ukraine. The United States has shipped tons of small-arms ammunition, mortar and artillery shells, Javelin antitank systems, Stinger anti-aircraft systems, and grenade launchers. Britain has delivered 3,615 antitank systems, as well as Starstreak antiaircraft missiles. The Baltic nations have sent antiaircraft missiles and antitank systems. Poland sent antiaircraft weapons. Turkey has delivered ground-attack drones. In a stunning reversal, Germany rushed 2,000 antitank weapons and 500 surface-to-air missiles to Ukraine. Non-NATO member Sweden delivered 5,000 antitank systems to Ukraine’s gallant defenders.

Challenges

Even so, Putin’s war on Ukraine has exposed challenges within NATO. The most glaring of these revolve around Germany – namely, Berlin’s equivocation over the future of the Russia-to-Germany Nord Stream 2 gas pipeline and Berlin’s decision to block delivery of German-built weapons to Ukraine. These policies prompted some observers to ask those eternal questions: “Is NATO broken, and is it worth the trouble?”

The answer to that first question is found in the above paragraphs. It’s impossible to read Putin’s mind, but the rapidity and unity of NATO’s response surely came as a surprise to the Russian strongman. Indeed, NATO’s response the past 70 days represents the very opposite of what happened when Putin mounted his first invasion of Ukraine in 2014.

The fact that NATO didn’t prevent Putin from moving against Ukraine isn’t a NATO failure; it’s a function of the harsh geopolitical reality that Ukraine is not a member of the most important, most enduring security alliance in history. To be sure, Europe will be more stable – and NATO more secure – if Ukraine can somehow remain a sovereign, democratically oriented nation. That explains why the alliance worked so hard on the diplomatic and military front to make Putin think twice about this criminal invasion.

However, the central purpose of NATO is to deter an attack against its members and, if necessary, to defend its members from attack. Indeed, the fact that Putin has attacked Ukraine while keeping his hands off NATO members Estonia, Latvia, Lithuania and Poland underscores that he respects NATO’s all-for-one security guarantee – at least for now.

In these weeks of war, Ukraine has shown itself to be a nation of warriors and a worthy ally. Its Churchillian leader and courageous people have earned NATO’s respect – and if they survive the hell Putin has unleashed, a seat at NATO’s table. But Russia's sheer mass could be enough to overwhelm Ukraine, especially as Putin employs the beastly scorched-earth tactics he perfected in Chechnya and Syria.

Headaches

As to whether the alliance is worth the headaches and heartburn it causes – especially for the United States – the answer to that question is found in both the historical record and today’s headlines.

To be sure, Germany’s prewar resistance to sending defensive weapons to Ukraine frustrated its NATO allies, and Germany's dependence on Russia’s natural gas has proven to be shortsighted. But it pays to recall that NATO overcame far more worrisome internal challenges in the past. Consider the Anglo-French deceptions during the Suez crisis in 1956, France throwing out NATO’s headquarters and pulling out of NATO’s integrated military command in 1966-1967, open hostilities between Turkey and Greece in the 1970s and 1980s, and France and Germany waging a diplomatic war against the United States and Britain in 2002-2003 over Iraq’s repeated violations of U.N. Security Council resolutions.

In spite of all of that, NATO repeatedly proves its importance to America’s security. Too many Americans forget or simply don’t know that NATO is a force-multiplier for U.S. power, a bridge to global hotspots, a backstop against great-power war in Europe, and a ready-made structure where like-minded nations with shared values and high levels of military interoperability build coalitions to defend their freedom and interests. These alliances within the alliance helped the United States liberate Kuwait, defend Saudi Arabia, wage war and keep peace in the Balkans, avenge 9/11, topple Saddam’s regime and respond to COVID-19.

Moreover, Germany has now suspended Nord Stream 2. As noted, Germany has rushed thousands of weapons systems to Ukraine. And in a truly remarkable about-face, Germany is increasing its annual defense outlays to 2% of GDP (something Washington and NATO have been begging Berlin to do since 2006), creating a $112.7 billion modernization and rearmament fund, and building a strategic LNG reserve and new LNG terminals.

“The world,” German Chancellor Olaf Scholz concludes, “will no longer be the same as the world before.” Or perhaps more accurately, Europe and the world are returning to what they were before 11/9, when the Berlin Wall collapsed.

Insurance

Throughout the post-Cold War period, the alliance served as an insurance policy, just in case Moscow reverted to its old ways. And here we are.

Insurance is a good way to understand NATO. Insurance, after all, is about providing protection against worst-case scenarios. Prudent people hope they never have to use insurance, but they realize that paying a little each month or each year protects them against having to pay a lot – or losing everything – if disaster strikes. The same is true in the realm of international security.

The deterrent represented by Article V of the North Atlantic Treaty serves as insurance against worst-case scenarios. For America, NATO is a hedge against another European conflict triggering another continentwide or worldwide war. For NATO’s other members, NATO is a security guarantee backed by America. Without that guarantee, there’s no security, as history has a way of reminding those on the outside looking in, from Cold War Hungary to post-Cold War Ukraine.

Like all insurance policies, there are costs associated with NATO. A recent study revealed that U.S. defense expenditures earmarked for Europe amount to $36 billion per year. That’s not a trivial amount of American taxpayers’ money. But consider what America gets in exchange for that insurance premium: a hedge against another Argonne or Normandy, a Europe reinforced against invasion, and economic benefits that exponentially exceed those premium costs.

With Putin trying to reconstitute the Russian Empire and reverse the settled outcomes of Cold War I, NATO is proving its worth yet again. As Gen. James Mattis puts it, “If we did not have NATO today, we would need to create it.”

#### The NATO Innovation Fund (NIF) and defense innovation accelerator (DIANA) are good first steps, but additional U.S. support is key to actualize their benefits.

Nelson 21 — Nicholas Nelson, Non-Resident Senior Fellow for Emerging Tech and Policy with the Transatlantic Defense and Security Program at the Center for European Policy Analysis, Senior Technology Advisor at the Georgia Tech Research Institute, 2021 (“Getting NATO Innovation Right,” Center for European Policy Analysis, June 18th, Available Online at https://cepa.org/getting-nato-innovation-right/, Accessed 07-03-2022)

The Defense Innovation Accelerator and NATO Innovation Fund announced at the NATO Summit are welcome developments, but they require new authorities and differentiated talent.

Swift technological change has meant governments and the military created new organizations and approaches to innovation and rapid acquisition. Unfortunately, many do not have the necessary authority, budget, or workforce to succeed, meaning that meaningful change and impact have been sacrificed for theater. For the newly announced Defense Innovation Accelerator North Atlantic (DIANA) – with planned locations in Toronto and Cambridge, UK – and the NATO Innovation Fund (NIF) to succeed, they must address authority and budget concerns, and then bring in the right personnel to lead and staff them.

Authorities

There are three key authorities that NATO must get right for DIANA and NIF: reporting lines, patience (or willingness to accept failure), and decision making.

\* First, DIANA and NIF should operate independently with a direct line into the most senior decision-makers (the Secretary General, SACEUR, Supreme Allied Commander Transformation — SACT, etc).

\* Second, they need to be allowed to fail. The most impactful defense organizations (and indeed commercial organizations, particularly in the startup world) normalize taking big bets, with the knowledge that many will likely fail, and even the ones that succeed may take years to realize their full impact.

\* Third and finally, these new NATO bodies need to invest in or provide support to initiatives and startups without requiring external permission or consensus. At the same time, they also need a clear transition partner for promising capabilities to be handed off to (e.g. DARPA transitioning tech to the U.S. Department of Defense), which can move from development to deployment. This will enable the Alliance to more readily identify, develop, and deploy emerging and disruptive technologies.

Similar efforts including the U.S. Department of Defense’s DARPA and Defense Innovation Unit, CIA’s In-Q-Tel, and USAF’s Strategic Capabilities Office, are effective because they exist outside of traditional bureaucracies, leverage non-traditional talent strategies, and have consistent budgets.

Budget

Allocating funding seems obvious, but too often limited forethought is given to this issue. To ensure success, organizational funding must be significant, multi-year, and consistent or include inbuilt annual growth. A number of high-potential initiatives have either been announced with no dedicated funding or have had sizable funding gaps in subsequent years damaging their brand and relationships with defense companies and startups alike. The NIF in particular will likely rely on the willingness of Alliance members to make contributions beyond other NATO obligations. If so, multi-year commitments are crucial, as are success metrics, such as return on investment, which are rarely used within NATO or national government departments.

Talent

Finally, and most overlooked, is getting talent right. External talent is crucial. It is not enough to simply construct new organizations staffed in the traditional manner. To realize their full potential, NATO must attract talent with startup and/or venture capital (VC) experience, and pair them with top subject-matter experts from R&D communities, both government, and commercial. This cannot be done with NATO’s current Byzantine, long, drawn-out hiring process, which can last six months or even longer, and advantage insiders versus external candidates. As such the Alliance must engage and attract this talent. The good news is NATO has a number of potential examples to draw on for potential hiring pathways. In the U.S. the Defense Digital Service hires design and technical experts for one-to-two “tours of duty,” using their skillsets and operate outside the traditional civil service. In the UK, strategy and technology professionals are seconded into the Ministry of Defence, the Department of Trade, and intelligence organizations such as GCHQ, to provide experience or skills that may not exist within the current civil service workforce.

But providing pathways alone is not enough: attracting this talent to apply and convincing them to join is just as important. This requires identifying areas where they might work, including industry, academia, and startups, and VC. At the same time, other steps are needed. Upskilling existing NATO civilians – among the international and international military staff (IS and IMS) — and Alliance service members are needed to address this skill and understanding gap. To do so, it is helpful to expose them to startup and VC environments. Programs like Shift’s Defense Ventures Program in the U.S. have succeeded in building understanding between the Department of Defense’s civilian and military workforce and startups and VCs. They’ve done so by bringing in high-performing defense personnel for eight-week immersions with growing venture-backed startups or VC firms. This cultivates the necessary connective tissue between startups, VCs, and the military. NATO could readily follow a similar process by providing its highest performers the opportunity to temporarily work alongside leading North American and European startups and investors.

What’s Next?

Accelerating the development, deployment, and integration of emerging and disruptive technologies into the strategic and tactical environments is at the core of future NATO operations. The Alliance’s move to build DIANA and NIF, along with incorporating the right language into strategic documents are significant first steps. But building these initiatives from scratch will require significant planning to establish the right authorities, budget, and talent environment to enable these organizations to thrive. In order to do so, they need to build outside of traditional NATO structures and models while creating a differentiated talent and organizational culture.

#### Specifically, increased U.S. security cooperation with NATO is vital to NIF and DIANA effectiveness.

Long 22 — James E. Long, Colonel in the United States Air Force, National Security Fellow with the Defense Project at the Belfer Center for Science and International Affairs at Harvard University, holds an M.S. in Space Studies from the American Military University, 2022 (“How the US Can Assist NATO and its European Alliance Members in Addressing the China Security Challenge,” Harvard University Belfer Center Defense Project Paper, June, Available Online at https://www.belfercenter.org/sites/default/files/files/publication/DefenseProject\_National%20Security%20Fellowship\_v3\_220624.pdf, Accessed 06-25-2022, p. 24-25)

4. The US should help NATO create R&D centers and defense innovation hubs to harness emerging technologies being developed by allies.

As was noted in the NATO 2030 Reflection Group, China is making rapid advancements in telecommunications, space, cyberspace, and other new technologies with the intent to be the world leader in AI by 2030 and the world’s leading global technological superpower by 2049.96 In response, NATO issued its 2030 Agenda that seeks to increase NATO transatlantic innovation and technological edge while preventing innovation gaps among allies.97 Moreover, the NATO Advisory Group on Emerging and Disruptive Technologies (EDT) issued a 2020 report citing pathways for NATO to become an EDT-ready organization, recommending that NATO establish a network of innovation centers [or defense innovation hubs] throughout NATO with funding to match.98

As a result, during the 14 Jun 2021 Brussels summit, NATO issued a communique announcing the establishment of a NATO Innovation Fund to promote transatlantic startups and a Defense Innovation Accelerator for the North Atlantic (DIANA). Since DIANA is intended to be NATO’s version of the US Defense Advanced Research Projects Agency (DARPA), the US is in a very good position to promote transatlantic coordination on AI, big-data processing, quantum-enabled technologies, autonomy, biotechnology, hypersonic weapons, and space.99 In addition, the US could support the Innovation Hub by helping pre-vet investors to ensure allied technology would be protected from illicit transfers.”100

Accordingly, the US should support NATO by helping create R&D centers and defense innovation hubs that could better harness emerging technologies to support NATO allies. These centers and hubs would help accelerate technology and improve cooperation among NATO allies and partners and would heavily rely on partnerships with academia, researchers, industry, and start-ups.101 Linked to these NATO centers and hubs would be universities, commercial [end page 24] sector, and allied countries’ organizations that accelerate technology into the hands of the warfighter. For example, the US has several organizations, such as DARPA, Defense Innovation Unit, AFWERX, SPACEWERX, Army Futures Command and NavalX, that could coordinate closely with NATO centers and hubs to collaborate on similar problem sets and solutions.

Another important facet of these NATO centers and hubs is assessing how the technology will impact NATO’s ability to jointly fight in the future. The NATO R&D Center would need to be linked to NATO’s Allied Command Transformation in Norfolk, Virginia, to identify potential impacts of the technology on NATO’s war-fighting capabilities. Accordingly, the US should work closely with NATO allies to ensure integration and interoperability with these new technologies.102

#### U.S. expertise and capabilities are key to quickly get required tech to the battlefield — U.S. cooperation will streamline NATO’s innovation pipeline.

Cook and Dowd 22 — Cynthia R. Cook, Senior Fellow and Director of the Defense-Industrial Initiatives Group at the Center for Strategic and International Studies, former Senior Management Scientist and Director of the Acquisition and Technology Policy Center at the RAND Corporation, holds a Ph.D. in Sociology from Harvard University, and Anna M. Dowd, Co-Founder of Digital Innovation Engine—an organization working on technology innovation, Adjunct Scholar at the RAND Corporation, former Principal Officer for Strategic Partnerships and Head of Industry Relations at the NATO Communications and Information Agency, former Fellow at the European Union Institute for Security Studies (France), holds an M.A. in International Relations from the Warsaw School of Economics (Poland) and a joint M.A. in European Studies from the Warsaw School of Economics (Poland) and Sciences Po (France), 2022 (“How to Get NATO Forces the Technology They Need,” *War on the Rocks*, May 13th, Available Online at https://warontherocks.com/2022/05/how-to-get-nato-forces-the-technology-they-need/, Accessed 07-12-2022)

In a Feb. 26 Twitter post, Mykhailo Fedorov, Ukraine’s vice prime minister and minister for digital transformation, asked the SpaceX chief executive, Elon Musk, to provide Ukraine with Starlink terminals to enable satellite-based communications. In less than 48 hours, Starlink user kits arrived in Ukraine, immediately improving the command-and-control ability of Ukraine’s military.

For those of us who study the NATO acquisition process, it is almost impossible to imagine the alliance identifying a requirement and adopting a solution so quickly, no matter how urgent the circumstances. Among the many challenges would be the alliance’s elaborate, consensus-based governing structure, as well as the divergent interests and funding mechanisms among the 30 member states. This is why, in 2016, the International Board of Auditors concluded that NATO struggles to provide commanders with required capabilities on time and estimated that common-funded capabilities required an average of 16 years from development to delivery.

The complexity of modern weapons systems and the challenges of interoperability mean that any active engagement will lead to the identification of new technical requirements for NATO. The alliance needs the processes and structures in place to rapidly identify these requirements and procure solutions. This includes giving commanders the authority to make decisions without the lengthy consensus-building approach that may be reasonable, if slow, in peacetime but is not effective during war.

First Steps

NATO has previously sought to improve the governance, speed, and efficiency of its capability-delivery process. For example, in 2018 NATO adopted a new governance model for common-funded capabilities. It has undertaken efforts to enhance collaboration between strategic commands (Allied Command Operations in Mons, Belgium and Allied Command Transformation in Norfolk, VA), called for the exploration of alternative acquisition strategies to support technology development, and created the Office of the Chief Information Officer to accelerate the delivery of computer and information systems. Furthermore, in October 2021 NATO launched the first $1.1 billion Innovation Fund, and last month announced the creation of the first ever Defense Innovation Accelerator for the North Atlantic to harness cutting-edge technologies as part of the NATO 2030 agenda.

These are valuable steps, but they do not address the fundamental challenge of rapidly acquiring common capabilities. There are still many residual processes where consensus-based control is inherently prioritized over speed, flexibility, innovation, and the deployment of prototypes at the end of their development phases.

NATO leaders recognize the ongoing challenge. In a recent speech to the North Atlantic Council, the supreme allied commander transformation, Gen. Philippe Lavigne, stressed that one of his key priorities is to ensure the timely delivery of new and critical capabilities, adding that “we need to change the rules and make them work for us, not against us.” But NATO leaders cannot fix this alone — the alliance’s 30 member nations are the ones that will have to agree on the solution. Exploring alternatives and getting the allies to agree on a solution will be difficult. It can happen on a NATO-wide basis, or some subset of member nations can take on the challenge and lead the effort, which may then be adopted by others.

What Works

Access to adequate funding is a necessary starting point, and NATO has a track record of funding common capabilities. In 2021, NATO was implementing over 3,000 common-funded projects, worth approximately $17 billion (of which the United States funds about 22 percent). These include providing critical technology that supports the planning and execution of all NATO air operations, and the Air Situation Data Exchange that enhances situational awareness at NATO’s borders with partner nations, including Ukraine.

But the capability-fielding process is still subject to delays, which would be dangerous when addressing needs identified during combat operations. To avoid this, alliance members should commit to providing funds for a rapid-acquisition organization on a preauthorized and discretionary basis, in essence creating a bank account that can be drawn upon when needed. Even if this were a credit line that members committed to, rather than a standing pot of funds, it would limit setbacks caused by the slow and political processes of identifying and appropriating funding.

Ensuring adequate funding is not the only answer. Commanders also need the authority to streamline the identification of urgent needs and a standing mechanism, not an ad hoc approach, that can provide the flexibility and authority to address them. This exists for some alliance members on a national basis. The commander of the Dutch Defense Materiel Organization’s Computer Emergency Response Team, for example, has a pre-authorized budget and the power to expedite acquisitions of up to 500,000 euros for urgent cyber capabilities within 14 days. However, there is no NATO-wide approach.

The U.S. Department of Defense offers a variety of acquisition approaches that NATO could draw from. The United States has a model where the military services are largely responsible for acquiring weapon systems and providing them to the joint force commanders. There are also several Department of Defense organizations that have been stood up to address cross-service challenges. This means that there are both joint department-wide and service-level acquisition organizations procuring materiel to serve as examples.

Over time, the Department of Defense has developed processes to allow requirements identified on the battlefield to be quickly addressed. Different parts of the department have also embarked on different forms of organizational innovation.

One example is the Air Force’s Rapid Capabilities Office, which was formed in 2003 to “expedite important, often classified programs while keeping them on budget.” The office has a unique management structure — it reports to a board of directors that is chaired by the undersecretary of defense for acquisition and sustainment and includes the most senior leaders of the Air Force and the under secretary of defense for research and engineering. These senior leaders can both set priorities for spending and work to find the necessary funding. Furthermore, acquisition experts at the Rapid Capabilities Office are carefully selected to maintain a culture where “lean, agile, and forward-looking technology development” is possible. Along with the Air Force’s new stealth bomber, the B-21 Raider, the office oversees the X-37B Orbital Test Vehicle, “an experimental test program to demonstrate technologies for a reliable, reusable, unmanned space test platform.” The effectiveness of the Rapid Capabilities Office is affirmed by the decision to put these two extremely important programs there rather than within more traditional Air Force acquisition organizations.

Another concept comes from the Defense Innovation Unit, which was designed to work across the Department of Defense to identify and understand critical national security challenges that can be solved with leading-edge commercial technology within 12 to 24 months. The Defense Innovation Unit connects with non-traditional suppliers in innovation hubs, including Silicon Valley, and uses flexible acquisition models to issue contracts in as little as 2 to 3 months. It then publishes a catalog of commercial “solutions” ready for purchase from a range of companies, many of whom are not traditional defense suppliers. These include the Next Gen Explosive Ordnance Disposal Underwater Response Vehicle, a remotely operated underwater vehicle that searches for mines, and Hunt Forward, a set of tools for forward-deployed cyber operations. Although implementation has not always been smooth, the Defense Innovation Unit has nonetheless provided battlefield commanders with a range of innovative solutions that they can turn to.

The Rapid Capabilities Office empowers its leadership to finalize requirements and rapidly commit funding, a crucial component of its success. The Defense Innovation Unit focuses on creating a pipeline of new technologies. And these organizations are not unique. There are others across the services, such as NAVALX, the Army Applications Lab, and AFWERX, that are aimed at adapting innovations from both traditional and non-traditional suppliers. The United Kingdom’s Royal Air Force has its own Rapid Capabilities Office, which has also shown promise.

These U.S. models prove that a bureaucracy as resistant to change as the Department of Defense can still develop new organizational structures and processes. The Dutch and British models show that attempts at organizational innovation are not limited to the Pentagon. NATO may choose to adapt one of these or to develop its own unique approaches. The goal should be to provide its commanders with the flexibility and the authority to “validate requirements” — that is, to formally approve what the warfighter needs to execute the fight — and to make resources available. The decision structure could be a small rotating board of senior leaders, perhaps with time limits for approving or rejecting requirements to force rapid decisions.

NATO also needs a way to connect with industry partners across the alliance, capitalizing on innovations from small businesses and startups using new and flexible contracting mechanisms. The alliance currently lacks the tools to rapidly adopt commercial technologies. Two related policies would help to enhance the ability of new technologies to connect with existing systems. To increase operational effectiveness, NATO should leverage interoperability standards that allow different systems to operate seamlessly in a multi-domain environment. A related approach would be to adopt open systems architecture approaches for NATO weapons. This would provide design information to companies for developing components that could work with existing systems using a “plug and play” approach. Both of these policies would build upon the traditional NATO strength of developing standards while making these standards relevant to innovative companies.

All these process changes and organizational innovations will take effort — and the journey may be slowed by NATO’s consensus-building culture. Transformation takes time, but it only begins when there is a clear case for change. The scale and scope of Russia’s attack on Ukraine provides that case, and the delivery of Starlink provides an example of what could be possible if NATO had a more flexible approach to acquisitions.

#### Integrating the U.S. and NATO’s EDT innovation networks is key to burden-sharing and interoperability — allies “say yes.”

Kliman and Thomas-Noone 18 — Daniel Kliman, Senior Fellow in the Asia-Pacific Security Program at the Center for a New American Security, former Senior Adviser for Asia Integration at the U.S. Department of Defense, former Senior Advisor at the German Marshall Fund of the United States, holds a Ph.D. in Politics from Princeton University, and Brendan Thomas-Noone, Research Fellow at the United States Studies Centre at the University of Sydney (Australia), former Research Associate in the International Security Program at the Lowy Institute (Australia), holds an M.A. in International Relations from the University of Melbourne (Australia) and an M.Sc. in Global Politics from the London School of Economics and Political Science (UK), 2018 (“Now is the time to take DIUx global,” *Defense News*, May 24th, Available Online at https://www.defensenews.com/opinion/commentary/2018/05/23/now-is-the-time-to-take-diux-global/, Accessed 07-11-2022)

The Defense Innovation Unit Experimental — the Pentagon’s signature effort to engage commercial technology startups ― is primed to go global. In fact, DIUx could become a key platform by which the United States and its allies and partners come together to address shared military challenges ― if its next managing director and supporters in the Pentagon and Congress are prepared to seize the moment.

Launched in 2015, DIUx reflected a growing realization that the U.S. military needs to more effectively leverage innovations developed in the commercial technology sector. Intended as a workaround to a sclerotic defense acquisitions process, DIUx came to rely on an obscure contracting authority to rapidly award prototype projects to innovative companies ― a welcome change to the Pentagon business models that never managed to align with the technology industry’s far faster pace.

By the end of the Obama administration, DIUx had expanded beyond Silicon Valley to two other U.S. innovation hubs — Boston and Austin.

Growth gave way to uncertainty following the 2016 presidential election, with observers questioning whether the new team would support DIUx, and Congress moving to restrict its access to funding. Since then, however, DIUx has won the support of key stakeholders. Secretary of Defense Jim Mattis visited DIUx in mid-2017 and offered an unequivocal endorsement of its mission to “accelerate commercial innovation to the war fighter.” Michael Griffin, the new undersecretary of defense for research and engineering, has also expressed backing for DIUx, which falls within his portfolio.

Congress has warmed somewhat to DIUx, though whether it will fund the White House’s requested plus-up remains uncertain. And DIUx has demonstrated its ability to do more than fund prototypes ― transitioning two projects into production contracts by the end of 2017.

Engaging commercial technology companies in the United States will ― and should ― remain the primary focus of the next DIUx managing director. However, with DIUx now on more solid political and bureaucratic footing, there is a unique opportunity to broaden its horizons.

Taking DIUx global could deliver multiple advantages. U.S. commercial technology companies do not hold a monopoly on innovations relevant to solving vexing military challenges. For example, Israel is a leading global provider of counter-drone solutions. A more internationally oriented DIUx could improve the U.S. military’s access to technologies generated by companies located on the soil of its allies and partners, and simultaneously enable their governments to more effectively harvest U.S. commercial technologies for national defense needs.

Many U.S. allies and partners would welcome the opportunity to plug into DIUx, given the diverse threats they confront ― from rising regional powers to terrorist networks ― and constraints on the resources they can dedicate to defense. At the political level, cooperation around DIUx could help strengthen America’s alliances and partnerships at a time of uncertainty, while also bolstering future military interoperability.

Looking ahead, the United States will need to identify new and innovative ways to share the burden with its allies and partners to maintain its technological advantage. Although the Pentagon will see a budget increase over the next two years, without legislative action, mandated budget cuts will return in 2020. A more internationally oriented DIUx could help to spread the costs of research and development. Over the long term, it could even evolve into the cornerstone of a commercial innovation-oriented defense technology network spanning the United States and its allies and partners.

With traditional forms of security cooperation like large-scale research and development projects and foreign military sales failing to keep pace with a rapidly evolving threat environment, such a network could enable the United States and its allies and partners to more effectively address shared national security challenges.

DIUx has taken limited steps to engage U.S. allies and partners. On the government side, these include welcoming a United Kingdom liaison officer and, reportedly, plans to host an Indian military representative. DIUx has also worked with a handful of foreign commercial technology firms.

Yet, beyond these initial steps, significant opportunity exists. To take DIUx global, the next managing director could pursue multiple, mutually reinforcing options.

The easiest would be for personnel from DIUx and the military services to conduct a series of roadshows to U.S. allies and partners. These roadshows would serve a dual purpose: to showcase the portfolio of U.S. firms that work with DIUx and to raise the awareness of DIUx among overseas companies that typically do not consider the Pentagon as a potential customer.

A second option would be to establish offices overseas in order to embed DIUx in key ally and partner innovation hubs. These offices could take various forms ― from a handful of DIUx personnel based in a U.S. embassy to a bilaterally staffed organization funded in part by the host nation.

DIUx offices overseas could function as points of coordination across U.S. alliances and partnerships, supporting efforts like the “Five Eyes” Technical Cooperation Program, but focus on technologies emerging out of the commercial sector in addition to national laboratories. Some key considerations for selecting a location would include a high density of companies working on cutting-edge technologies with national security relevance; commitment by ally and partner militaries to leverage technology developed in the commercial sector; and willingness of ally and partner governments to put up resources.

A third option would be to launch dedicated funds under DIUx with financing contributed from both the United States and its allies and partners to solve joint challenges. Each fund would focus on awarding prototype projects to companies with potential solutions to the challenge identified. This option would allow the United States and its allies and partners to share defense resources; provide more revenue to national security-relevant startups than the Pentagon could on its own; and build interoperability up front. A clear area for such a fund would be low-cost intelligence, surveillance and reconnaissance coverage over a vast maritime area ― a challenge that has long bedeviled the United States and Australia in the Indo-Pacific region.

The next managing director of DIUx will have an unparalleled opportunity to take it global. But she or he will need a mandate to do so ― ideally from the secretary of defense. With that mandate, the next managing director should quickly move to advance an ambitious agenda for involving allies and partners more closely in the work of DIUx. Announcing that DIUx will open an office overseas within a year would, in particular, galvanize ally and partner interest.

### 1AC — Plan

#### The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization to strengthen defense innovation hubs and research and development in artificial intelligence, biotechnology, and cybersecurity, including by substantially increasing its support for and participation in the NATO Innovation Fund and Defense Innovation Accelerator for the North Atlantic.

### 1AC — Alliance Fragmentation Advantage

#### Contention Two: Alliance Fragmentation

#### Current transatlantic EDT policy is fragmented — bridging the gap between the U.S., NATO, and the EU is key to effective innovation and interoperability.

Speranza and Jans 21 — Lauren Speranza, Director of the Transatlantic Defense and Security Program at the Center for European Policy Analysis, former Deputy Director of the Transatlantic Security Initiative at the Atlantic Council, holds an M.A. in International Security from the Brussels School of International Studies (Belgium), and Karlijn Jans, Defence Policy Advisor at the British Embassy in The Hague (Netherlands), former Strategic Analyst at the The Hague Centre for Strategic Studies (Netherlands), holds an M.A. in European Studies from King's College London (UK) and an M.A. in European Studies from the Humboldt Institute of Berlin (Germany), 2021 (“Bridging the Gap: Time for an EU-NATO Strategic Dialogue on Defense Tech,” Center for European Policy Analysis, February 17th, Available Online at https://cepa.org/bridging-the-gap-time-for-an-eu-nato-strategic-dialogue-on-defense-tech/, Accessed 07-10-2022)

To stay secure, the transatlantic community must take on emerging and disruptive technologies together.

Today’s transatlantic security hinges on technology. On both sides of the Atlantic, our militaries, societies, economies, and information systems require increasingly advanced technologies to stay better, faster, and stronger than our adversaries and competitors. To retain their advantage and address vulnerabilities, the United States and Europe must work in lockstep to harness emerging and disruptive technologies for their collective defense. The key is to employ NATO and the European Union (EU) in unison for strategic effect.

NATO, the EU, and their member states have recognized the urgent need to combine their complementary capabilities to contest Russia and China, especially in the technological domain. Just yesterday, NATO Secretary General Stoltenberg announced a new a Defense Innovation Initiative “to promote interoperability and boost transatlantic cooperation on defense innovation” among allies – 21 of which are members of both NATO and the EU. NATO and the EU also share an overlapping set of forces, capabilities, talent, intellectual property, and budgets for defense investment and research and development (R&D). Under the 2016 Joint Declaration, practical NATO-EU cooperation has been humming along, despite lingering political obstacles. Applying emerging and disruptive technologies (EDT), such as artificial intelligence (AI), autonomous systems, space capabilities, hypersonics, quantum tech, and human augmentation, for defense has been a key focus area. This has been underscored by, for example, jointly supported workshops at the European Center of Excellence for Countering Hybrid Threats (Hybrid COE) and NATO-EU senior military staff talks. As each organization has made EDT advances, staff-level coordination and broad information sharing have helped to better align their efforts. For instance, NATO’s EDT roadmap team, Innovation Hub, and Science and Technology Organization have engaged with the European Defense Agency (EDA)’s tech work.

But staff-level coordination can only bear so much fruit in the absence of a more robust political effort. As strategic and technological competition with Russia and China has intensified, the stakes have risen too high to settle for incremental activities. Avoiding the political battles required to forge a more meaningful joint NATO-EU approach, nations have begun exploring other transatlantic forums to address EDT issues. The Canadian and French-led Global Partnership on AI, the U.S.-led AI Partnership for Defense, and the European Commission’s proposed Transatlantic Tech and Trade Council are a few examples. Each of these platforms is useful in its own right, specifically for AI issues, and could benefit from NATO and the EU joining to add their institutional weight. The risk with this approach, however, is the rapid fragmentation of transatlantic efforts on EDT. If this trend continues, the result could be a diffused smattering of multilateral frameworks, each focused on a particular tech issue with a different small group of countries.

By opting for outside platforms, the transatlantic community misses the point. The added value of NATO and the EU is their ability to coordinate efforts among large groups of like-minded nations. Both institutions have a great deal of experience and infrastructure for doing so. On a transformative set of issues that requires a comprehensive approach, such as the defense application of EDT, NATO, and the EU have the capacity to make an enormous collective impact. Instead of scattering across alternative forums, interested member nations must find ways to drive their EDT work through a new NATO-EU mechanism.

Launching an EU-NATO Strategic Dialogue on EDT could be an important option to explore. Routine, higher-level meetings in this format would draw together senior representatives from each institution, as well as member states and the private sector — each of which plays vital roles in assessing vulnerabilities and shaping requirements for EDT. The scope should expand beyond AI alone to encompass consultations on the wider security implications of EDT. Tentative agenda items could include forging key principles for tech governance around the military applications of EDT; addressing data-sharing issues; coordinating defense R&D and investment incentives; and establishing more robust standards and technical requirements for EDT-enabled systems to enhance interoperability. This could potentially have positive spillover in better aligning EDT aspects of the EU Capability Development Plan (CDP), the Coordinated Annual Review on Defense (CARD), and the respective NATO Defense Planning Process (NDPP). It would also create synergies for the EU to leverage its budgetary and legislative tools, which NATO lacks, to more effectively reinforce the Alliance. Lastly, it could strengthen the collective “annual review of vulnerabilities in alliance critical infrastructure and technologies, including those stemming from foreign ownership and influence”, as the NATO Secretary General has proposed.

The plethora of applications of emerging and disruptive technologies in the defense realm is something that both militaries and policymakers are dealing with on a daily basis. Developments are rapid but, at the same time, require long-term engagement and vision from senior leaders. In the end, EDT not only has implications for soldiers on the battlefield, but also for political decision-makers. In the near term, the COVID crisis is occupying much of the bandwidth and institutional capacity across NATO and the EU, at the expense of accelerating the dialogue in support of defense innovation. But urgent action is needed to grow the transatlantic community’s fast-shrinking technological advantage in defense. It is paramount for leaders to diligently and intensively focus on this topic, as opposed to simply including it on the long list of issues for NATO or European Council meetings. Through a structured EU-NATO Strategic Dialogue on EDT, it could rightly become an integral part of the transatlantic meeting cycle, not least to create a common understanding around future defense implications. To this end, the NATO 2030 Reflection Group’s proposed NATO digital summit for governments and the private sector should be extended to EU stakeholders and ultimately feed into this strategic dialogue.

To stay secure, the transatlantic community must take on emerging and disruptive technologies together. It should be at the forefront of the joint action by the EU and NATO, reflecting the pressing need to act. This is of foundational importance for maintaining the Alliance’s strategic edge, addressing vulnerabilities of tech, and defending the norms and values it was built to protect. As the United States and Europe renew their collective agenda at the dawn of the new Biden administration, an EU-NATO Strategic Dialogue on Defense Tech should be at the top of their list.

#### Insufficient U.S. support for NIF and DIANA is driving this fragmentation — the plan is key to supercharge NATO-EU cooperation on EDT.

Besch 21 — Sophia Besch, DAAD/AICGS Research Fellow at the American Institute for Contemporary German Studies at Johns Hopkins University, Senior Research Fellow at the Centre for European Reform (Germany), Non-Resident Senior Fellow at the Atlantic Council Europe Center, Ph.D. Candidate in European Studies and Defence Studies at King's College London (UK), holds an M.Sc. in International Relations from The London School of Economics and Political Science (UK) and an M.A. in International Security from Sciences Po (France), 2021 (“Rebooting the U.S.-EU Defense Relationship,” American Institute for Contemporary German Studies, December 22nd, Available Online at https://www.aicgs.org/publication/rebooting-the-u-s-eu-defense-relationship/, Accessed 07-10-2022)

2. Align EU-NATO work on defense innovation and find new formats of engagement

Both the United States and the EU have an interest in investing in new and emerging defense technologies and to maintain interoperability, particularly in the context of the U.S. technology race with China. The United States, through AUKUS, has established an innovation partnership with just one European ally, the UK (for now). Meanwhile, NATO has launched a new defense innovation fund and a defense innovation accelerator (DIANA). The UK, which post-Brexit has given itself the guidance to ‘Think NATO,’[7] was a supporter of the Fund, but the United States and France are not members. At the same time, France often argues that the EU should be in the lead on emerging technologies and is pushing for the creation of an Innovation Defense Hub within the European Defense Agency. These defense innovation efforts pursued in parallel by both organizations are already leading officials to complain about NATO duplicating the EU and vice versa. Both Americans and Europeans should try to prevent a rehashing of this unproductive talking point.

Parallel to the EU branching out into ‘traditional’ security, NATO has been broadening its own understanding of security to include newer domains such as economic security, disruptive technologies, and disinformation.[8] This development provides clear opportunities for cooperation between the two organizations, but also presents risks of conflict and tension. NATO-EU cooperation today remains largely process-driven. Inter-institutional exchanges are often focused on ‘deconflicting’ rather than building genuine synergies,[9] and the relationship suffers from long-standing political conflict between Turkey and Cyprus and from newer tensions between the UK and France. The concurrent NATO Strategic Concept and EU Strategic Compass processes are an opportunity for the United States and the EU to work together to improve NATO-EU cooperation on innovation. The next NATO-EU joint declaration, which is scheduled to be published soon, could help by acknowledging a new division of labor between the two institutions.

For instance, it would make sense for the two organizations to cooperate on investment screening, research protection, and initiatives to facilitate information-sharing on dual-use export and import controls of critical technology.[10] These joint NATO-EU initiatives could usefully build on the work done by the United States and the EU at the Trade and Technology Council. On defense technology development, the Americans and Europeans could explore different new formats of engagement. For instance, the United States could expand AUKUS to include more European countries with relevant defense innovation profiles, such as France or Estonia. Or, if AUKUS remains too politically sensitive for Paris, the transatlantic allies could explore the possibility of the United States joining selected PESCO projects geared towards defense innovation. The United States may also want to reconsider its decision not to join DIANA.

#### U.S. support and participation is key to overall alliance coordination on EDT.

Mundell 22 — Ian Mundell, Innovation Reporter at *Science|Business*—a network of universities, companies, and research and policy organisations promoting innovation, 2022 (“The Ecosystem: in Europe, defence innovation is the new black,” *Science|Business*, June 7th, Available Online at https://sciencebusiness.net/news/ecosystem-europe-defence-innovation-new-black, Accessed 07-03-2022)

Suddenly, it seems, everyone cares about Europe’s defence innovation ecosystem. NATO is setting up the Defence Innovation Accelerator for the North Atlantic, or DIANA, with a significant presence in Europe. The European Commission is working on the EU Defence Innovation Scheme, EUDIS. And last month, Amazon Web Services announced it is setting up a private defence accelerator in the UK.

But details of the DIANA and EUDIS initiatives have been slow to emerge, leading to concerns that gaps and barriers to innovation remain to be addressed. EUDIS in particular leaves a lot of questions unanswered.

“It’s a step in the right direction, but whether it is enough is deeply debatable,” said Nicholas Nelson, senior fellow with the Transatlantic Defense and Security Program at the Center for European Policy Analysis in Washington DC. “And this will not be figured out in the next year or two. It will take five or ten years to see what the impact is.”

This sentiment is echoed by Alain De Neve, a specialist in defence innovation at Belgium’s Royal Higher Institute for Defence. “EUDIS is a timely initiative for the EU member states, although from a macro-strategic point of view there is still a long way to go for Europeans if they want to build a competitive research ecosystem on a more global scale,” he said.

Detecting hidden threats

EUDIS is intended to bring together all relevant EU initiatives that support defence innovation and entrepreneurship. This includes innovation-focused calls for proposals issued through the European Defence Fund (EDF), such as a planned technological challenge to test and mature technologies for hidden-threats detection, and a four-year partnership for the development of defence medical counter measures against chemical, biological, radiological and nuclear threats.

The Commission also plans a number of initiatives intended to structure the European defence ecosystem. Some of these are still frustratingly vague. There is to be a dual-use incubator to allow better spin-in and spin-out between the civil and defence sectors, and to spur technological maturation and adaptation. This project was first floated in the EU’s 2021 Action plan on synergies between civil, defence and space industries, which suggested it might be a virtual network based on close collaboration between the Commission, the European Innovation Council and the European Defence Agency.

At that stage, the incubator’s potential activities included screening EU-funded research for results relevant to defence and proposing them for follow-up funding or user uptake. It was also to support new technologies with dual-use potential coming from start-ups, SMEs, and research and technology organisations. But these details and partners have vanished from the latest description of the incubator, and the Commission says it has nothing more to add while preparations are on-going.

Detail is also still lacking on the cross-border innovation networks listed as part of the EUDIS toolbox. These are intended to test the relevance of technologies from the civil sector in defence-specific environments. Then there will be other supporting measures for innovative companies, such as matchmaking with primes, investors and end users; business coaching; and the organisation of hackathons.

Defence Equity Facility

The most concrete EUDIS initiative unveiled so far is the Defence Equity Facility, which is intended to address the lack of risk capital in the EU for start-ups and small and mid-size companies developing innovative defence technologies. The Commission will put €100 million into the facility over the next five years, which is expected to be augmented by the European Investment Fund and private investors to reach a total of €500 million.

“Enabling a better access to equity funding for innovative defence SMEs and mid-caps would support their growth and finally benefit to the innovativeness of the European defence technological and industrial base,” the Commission says in the latest EDF work programme, released on 25 May. “It will also reduce their exposure to non-EU investors and benefit to the EU’s strategic autonomy.” The creation of the facility is also intended to send a positive message to private investors that the EU’s defence sector is an attractive proposition.

Nelson thinks the Defence Equity Facility is a good start, but again a lot of important detail is still missing, such as how and on what terms the equity will be awarded. An enlightened choice would be to make non-dilutive investments, the approach used by Air Force Ventures in the US. “It is not taking equity, it is investing alongside private capital investors, because it views this as good for the ecosystem,” Nelson said.

But Nelson is also concerned that the facility potentially appears open to all-comers, rather than targeting start-ups and companies with a civilian background moving into defence. If confirmed, this will limit its impact.

For example, a seed round for a defence start-up might typically be around €2 million, with €500,000 from the Commission contribution required to lead the round. So, if the facility is focused exclusively on this early stage investment it might support 40 companies a year, which is modest enough. But if the facility gets involved in series A and B rounds, which might run to €5-7 million per round, its reach will be severely constrained. “To be honest, it needs to have another zero on the end per annum to have a catalysing effect,” said Nelson.

Gundbert Scherf, co-founder and managing director of Helsing, a German start-up active in artificial intelligence and software-defined defence, thinks this lack of focus is already holding back EDF. “Only 8% of EDF funds to date have been allocated to disruptive technologies. Consortiums primarily feature traditional primes instead of deep tech disruptors, who actually invest their own money into de-risking tech and hiring the right talent,” he said. “In reality we need to spend the majority of funds on disruptive technologies and empower new defence companies that are developing them. Only this will deliver the innovation, disruption, speed, and quality we need.”

Dual-use technologies

Another aspect of EUDIS that is unclear is how it will line up with NATO’s DIANA initiative. This was launched in April, with a mission to bring industry, start-ups and academia together to research new dual-use technologies. Initially it will run a network of more than 10 accelerator sites and over 50 test centres in innovation hubs across NATO alliance countries. The UK and Estonia will host DIANA’s European accelerators. Meanwhile, a complementary NATO Innovation Fund will invest €1 billion in early stage start-ups and other deep tech funds, over an unspecified period of time.

The Commission says that it will work with NATO “to ensure that we can develop synergies when and where possible”. De Neve thinks this may not be so straightforward. “It would be difficult to imagine that these two cooperation frameworks could operate without any exchange between them,” he said. “However, and to the extent that DIANA assumes the contribution of the US, it seems difficult to imagine interactions between these two institutions that do not clash with the restrictive measures put in place by the US in terms of transfer of sensitive technologies.”

#### U.S. security cooperation *with NATO* on EDT is vital to cement an alliance-centric framework that links transatlantic *and* Indo-Pacific allies.

Ford and Goldgeier 21 — Lindsey W. Ford, David M. Rubenstein Fellow in Foreign Policy at the Brookings Institution, Adjunct Lecturer in the Elliott School of International Affairs at George Washington University, former Richard Holbrooke Fellow and Director for Political-Security Affairs at the Asia Society Policy Institute, former Special Assistant for the US-ASEAN Defense Forum in the U.S. Office of the Secretary of Defense, holds an M.A. in Public Affairs and Asian Studies from the University of Texas-Austin, and James Goldgeier, Visiting Fellow in the Center on the United States and Europe at the Brookings Institution, Professor of International Relations at American University, former Professor and Director of the Institute for European, Russian, and Eurasian Studies at George Washington University, former Director for Russian, Ukrainian, and Eurasian Affairs at the U.S. National Security Council, holds a Ph.D. in Political Science from the University of California-Berkeley, 2021 (“Retooling America’s alliances to manage the China challenge,” The Brookings Institution, January 25th, Available Online at https://www.brookings.edu/research/retooling-americas-alliances-to-manage-the-china-challenge/, Accessed 07-10-2022)

Beyond building collective capacity to operate more seamlessly in response to today’s crises, the U.S. must also think more closely about building alliance innovation ecosystems for the future. With China set to overtake the U.S. in research and development spending — it already spends more on R&D than Japan, Germany, and South Korea combined — the U.S. and its allies will need to treat defense innovation as a combined task. Rising techno-nationalism and the lack of allied innovation networks will make this difficult absent intentional policy leadership. Looking forward, Washington should further expand new bureaucratic mechanisms such as allied R&D pools or defense innovation hubs that could better harness emerging technologies being developed across allied capitals. While the Defense Department is focused on initiatives that will improve America’s sclerotic acquisition and innovation processes, these efforts need an alliance-centric approach from inception, rather than treating allies as an add-on to existing American plans. NATO, for example, might consider establishing an allied version of the Defense Advanced Research Projects Agency (DARPA), in which key allies could collaborate on emerging technologies, as proposed by the 2017 GLOBSEC NATO Adaptation Initiative. Indo-Pacific allies such as Australia, Japan, and South Korea could be incorporated in this initiative through their role as NATO “global partners.”

#### NATO leadership and Indo-Pacific allied cooperation on EDT innovation is key to counter China.

Nouwens 22 — Meia Nouwens, Senior Fellow for Chinese Defence Policy and Military Modernisation at the International Institute for Strategic Studies (UK), Co-Leader of the China Security Project at the Mercator Institute for China Studies (Germany), holds an M.A. in International Relations and Diplomacy from Leiden University (Netherlands) and an M.Phil. in Modern Chinese Studies from the University of Oxford (UK) and Peking University (China), 2022 (“NATO and Digital Cooperation with the Indo-Pacific,” German Marshall Fund of the United States, February 11th, Available Online at https://www.gmfus.org/news/nato-and-digital-cooperation-indo-pacific, Accessed 07-07-2022)

Meeting the Challenge: Digital Technologies

Due to the nature of the challenges that China poses to it, NATO’s priority should be to meet them at home. However, in countering the economic, technological, and security challenges that China poses, collaboration with partner countries in the Indo-Pacific that are like-minded and have valuable experience in countering Beijing’s assertiveness is equally important. Nevertheless, as Secretary General Stoltenberg has stated, NATO is unlikely to face the China challenge by being physically present in the South China Sea or elsewhere in the Indo-Pacific region.25 to resource constraints and other concerns, this remains unlikely in the near future. NATO can best meet the technological challenge that China poses through greater collaboration and coordination with regard to the digital space and emerging and disruptive technologies. While current NATO activity in EDTs, as well as in data management and governance, is a step in the right direction to protect domestic resilience and to enhance innovation capacities, there are further options to strengthen the alliance’s technological edge at home and with partners in the Indo-Pacific.

Expand NATO collaboration on EDTs to partners in the Indo-Pacific

NATO is in the process of developing the mechanisms, funding, and strategy behind DIANA and the NATO Innovation fund, the former aimed at launching in 2023 and the latter potentially totaling to $1 billion. DIANA aims to be NATO’s version of the United States’ Defense Advanced Research Projects Agency and to bring together transatlantic efforts on critical technologies, working with industry and academia on AI, big-data processing, quantum-enabled technologies, autonomy, biotechnology, hypersonic weapons, and space. Subsequently, the Innovation Fund will seek initially to invest $81.2 million per year in transatlantic startups. Importantly, it will work with pre-vetted investors to ensure that “the technology will be protected from illicit transfers.”26

While much is still left to be decided on both these efforts, there are clear areas for practical cooperation with partners in the Indo-Pacific; for example, with regard to the Australia-United Kingdom-United States (AUKUS) security pact and the Quadrilateral Security Dialogue joining Australia, India, Japan, and the United States.

First, AUKUS aims to promote cooperation beyond the initially agreed nuclear-powered-submarine program. The agreement seeks to foster “deeper integration of security and defense-related science, technology, industrial bases and supply chains.”27 Trilateral collaboration will focus on cyber capabilities, AI, quantum technologies, and additional undersea capabilities.

Following the first in-person leaders’ summit of the Quad in September 2021, leaders of the four countries put forth an initiative to partner on emerging technologies, space, and cybersecurity, and to cultivate next-generation talent.28 Exact timelines for these initiatives are still unclear. With regard to the latter, the Quad Fellowship will provide 100 scholarships per year for students in science, technology engineering, and mathematics from the four countries to study in the United States. Ultimately, the program will seek to develop a network of science and technology experts among the Quad countries. On critical and emerging technologies, the countries will work together to publish a statement of principles that touches on the design, development, governance, and use of technology; to establish a technical standards contact group; to launch a semiconductor supply-chain initiative; to support 5G deployment and diversification; and to monitor advances in biotechnologies.29 The Quad countries will also collaborate on cybersecurity issues and establish a space-related working group that shares climate change-related satellite data, enables capacity-building in space-related domains in other Indo-Pacific countries, and consults on norms and guidelines.

While the overlap is not exact, there are significant areas for cooperation between NATO, AUKUS, and Quad countries. Australia and Japan are already NATO partner countries and cooperate politically with the alliance on a variety of levels from parliaments to heads of state, ministries of foreign affairs and defense.30 **[[[\*\*\*Start Footnote 30\*\*\*]** NATO’s “global partners,” such as Australia and Japan, are countries with whom the alliance engages politically and have access to the same activities that NATO Individual Partnership Cooperation Programme countries receive. They work with NATO on areas of common interest, such as cyber defence, counterterrorism, non-proliferation, and resilience. In some cases, NATO and its global partners cooperate through NATO military operations or through defence capacity, training, and educational programmes. See NATO, Relations with partners across the globe, August 25, 2021. **[[[\*\*\*End Footnote 30\*\*\*]]]** Bringing partner countries into NATO’s programing on EDTs would not only increase the alliance’s innovative capacities but also allow it to align itself with the priorities of partners in the Indo-Pacific to a greater extent.

A potential stumbling block for such cooperation might be the recent tensions between the EU (and therefore some NATO members) and the AUKUS countries. Transatlantic relations soured following the announcement of the establishment of the security pact and the related cancellation of the submarine deal worth $90 billion between Australia and France. The announcement of AUKUS also coincided with the publication of the EU’s Indo-Pacific strategy, which highlights the ambition to work with the Quad in the region.31 There is thus a potential risk that EU members that are also NATO members, in particular France, may prioritize technological development within an EU rather than NATO context.

This risk may be overstated, however. The EU’s Indo-Pacific strategy focuses primarily on digital governance and partnerships: the development of shared technological standards, alone and together in coordination with like-minded partners, for areas such enhancing governance around AI based on democratic principles and fundamental rights. The EU’s practical engagement with its Indo-Pacific partners on the development of EDTs is still limited. It only has agreements on areas of practical cooperation and development with a select few countries in the Indo-Pacific, such as India and Japan with which it has agreed to deepen cooperation on 6G, standardization, AI, blockchain, and quantum and other technologies.

Second, the security and defense section of the EU’s Indo-Pacific strategy does not make any mention of cooperation with like-minded countries in the Indo-Pacific on EDTs. The strategy’s main focus here is on cooperation on disinformation, maritime security, outer space, cybersecurity, peacekeeping, counterterrorism, and arms control. As the EU’s focus on EDTs is primarily on standard setting, governance, ethics, and civilian applications, there may be an opportunity to collaborate and share the burden with NATO. NATO could work alongside the EU to ensure standards are set for EDTs in the defense and civilian realms while taking the lead on the development and adoption of defense-related EDTs.

Establish NATO standards on data governance together with partners in the Indo-Pacific

In 2017, the commander of NATO’s Allied Command for Transformation, General Denis Mercier, stated that “data is now a main strategic resource. Processes for collecting, sharing, exploiting and distributing data are the main drivers to adapting organizations.”32 This remains true with regard to the military and civilian, public and private sectors. If shared policies on data governance promote interoperability, help to establish rules and norms, and secure data, then divergent policies could have the opposite effect. If NATO aims to remain competitive and to increase its innovation strengths in EDTs and digital technologies, digital policy coordination should be an area of discussion within the alliance.

In October 2021, NATO defense ministers agreed to the alliance’s first-ever strategy for AI, which includes an ambition to agree on standards of data collection and use for AI. NATO also has standards and processes related to big data produced by the alliance.33 However, if NATO members and partner countries seek to cooperate and collaborate on the development and adoption of emerging technologies and data-driven innovation, then addressing data governance and trusted cross-border data flows between allies and across partners is of importance. To date, some NATO members are aligned through membership of the EU and its General Data Protection Regulation (GDPR) and through the European Data Governance Act (subject to final approval by the European Parliament and Council of the EU this year).34 However, other allies, such as the United States, have taken different approaches to data governance and it remains to be seen whether the new EU-US Trade and Technology Council can find solutions for transatlantic cooperation in this area.35

Last, if collaboration between the innovative economies of NATO allies and their partners in the Indo-Pacific is a goal, then greater like-mindedness and alignment of data-governance norms should be an area of consideration in the future within the alliance and with countries like Australia, India, and Japan.

This undoubtedly falls outside of the realm of NATO’s traditional area of competence and more clearly a suitable role for the European Commission. This is not an obstacle: NATO has agreed already to work with the EU in areas where the latter has experience and competence. Furthermore, the EU is an active player in bilateral discussions between member states and non-EU countries about data sharing and data governance. Its Indo-Pacific strategy already envisions a greater role for the EU in the region in areas of digital governance through Digital Partnership Agreements with Japan, Singapore, and South Korea. The EU has already deepened its digital partnership with India in 2021 which seeks to promote 5G in line with global strategies and develop joint visions for next generations of information and communications technology, to promote digital cooperation between private sectors in each country, and to ensure that data regulation in India and the EU align with each other. Similarly, the EU and Japan created the world’s largest area of safe data flows in 2019 when the European Commission adopted an adequacy decision on Japan for a data-sharing agreement.36

Conclusion

While countering the challenges that China poses to NATO will not be easy, the greatest challenge will be to find agreement and unity between allies on how to address their shared concerns about China’s rise. The limitations on NATO’s resources, particularly due to the requirements of allies to focus on collective security and defense at home, will make it difficult for the alliance to counter the China challenge in the Indo-Pacific. Though a show of commitment by sending military assets to the region and NATO’s partners there is important, addressing the challenges that China poses to the alliance and its partners alike should be done in more varied ways.

NATO should focus on expanding its current work in the digital sphere to cooperation and collaboration with partner countries in the Indo-Pacific in order to build a strong ecosystem of like-minded digital actors. By cooperating on EDTs and sharing data to ensure that the private and public sectors in allied and partner countries as well as institutions like the EU remain competitive, NATO and like-minded countries can take steps toward bolstering their defense and security capabilities and preparing for competition as well as for conflict.

#### Failing to effectively counter China causes war — we’re on the brink.

Colby 22 — Elbridge Colby, Co-Founder and Principal of The Marathon Institute—a policy initiative focused on developing strategies to prepare the United States for an era of sustained great power competition, Member of the Council on Foreign Relations, former Director of the Defense Program at the Center for a New American Security, former Deputy Assistant Secretary of Defense for Strategy and Force Development at the U.S. Department of Defense, Recipient of the Distinguished and Exceptional Public Service Awards from the U.S. Department of Defense and of the Superior and Meritorious Honor Awards from the U.S. Department of State, holds a J.D. from Yale Law School, 2022 (“China, Not Russia, Still Poses the Greatest Challenge to U.S. Security,” *The National Interest*, July 1st, Available Online at https://nationalinterest.org/feature/china-not-russia-still-poses-greatest-challenge-us-security-203228, Accessed 07-12-2022)

American foreign policy after—indeed, during—the Russo-Ukrainian War should promptly head to the world’s most decisive region: Asia. This will require that American foreign and defense policy genuinely put Asia first—in our military investments, in our allocation of political capital and resources, and in our leaders’ attention.

Nothing that has happened since Russia’s abominable invasion of Ukraine has changed a set of facts: Asia is the world’s largest market area, and it is growing in global share. Located in the middle of Asia is China which, alongside the United States, is one of the world’s two superpowers. China’s behavior has become increasingly aggressive and domineering and appears oriented toward establishing Beijing’s hegemony over Asia. If Beijing achieves this goal, the resulting consequences for American life will be dire.

Preventing China from establishing this hegemony over Asia must therefore be the priority of U.S. foreign policy—even in the face of what is happening in Europe. The simple fact is that Asia is more important than Europe, and China is a much greater threat than Russia. By way of comparison, Asia’s economy is roughly twice as large as Europe’s today—but within twenty years it will likely be multiple times greater. China, in the meantime, has a GDP roughly an order of magnitude larger than Russia’s.

If current trends continue, China appears on a trajectory to achieve its hegemonic ambitions. Beijing has been building a military distinctly not limited to territorial defense. Rather, it will be capable of enabling Beijing’s pursuit of much larger and ambitious goals—first by ingesting Taiwan, but not ending there. Indeed, amidst the furor over the war in Ukraine, Beijing announced yet again that it would increase its defense spending by 7 percent this year. Meanwhile, despite much talk, the United States has neglected its military position in Asia, while many of its allies—especially Japan and Taiwan—have been laggard in maintaining their defenses. As a result, the military balance in Asia has continued to shift markedly against the United States and our allies. In blunt terms, we are now rapidly approaching, if not already in, the window of opportunity where China might well decide to attack Taiwan—and we might lose.

Avoiding this outcome must be the top, overriding priority for U.S. policy. This does not mean Europe is unimportant or that we should neglect or abandon it. We should actively support Ukraine with weapons and other forms of support while remaining firmly committed to NATO, albeit with our contributions being more focused and narrow in scale. But it does mean Asia must be our priority, and genuinely so, not just rhetorically as has so often been the case in the past.

Because of these factors, shifting our focus to Asia would make sense regardless of how Russia’s invasion of Ukraine fared. But, if anything, the war in Ukraine and the reaction to it has made it even more palatable for the United States to turn to Asia. Moscow, while still menacing and dangerous, has vividly demonstrated that its power is less formidable than many of us had feared. Russia is very likely to try to recover its strength, but the losses of war and the impact of sanctions are likely to make that process slow and difficult. At the same time, Europe has stood up, announcing major increases in defense spending, supporting Ukraine’s own self-defense, and demonstrating an unprecedented degree of cohesion in applying sanctions and other forms of pressure on Russia.

The result is that Moscow appears less of a threat than many of us had supposed, while Europeans are doing more to shoulder their own defense. If anything, this should make the United States more, not less, ready to focus on Asia. Indeed, in these circumstances, it is actually hard to understand the logic of increasing America’s focus on Europe. Why would we double down in Europe at the expense of Asia when there is less of a threat from Russia and more European self-help—all while the danger in the primary theater only increases?

Yet many in the foreign policy and political elite seem to view the Russo-Ukrainian War as an opportunity precisely to double down in Europe. Even more, for some, it is a chance to try to turn the foreign policy clock back to the globe-spanning liberal imperialism of two decades ago.

Washington must resist this temptation like the plague. The breathtakingly hubristic foreign policies of the 2000s were unwise even in the period of unipolarity, as we have found to our chagrin. As American leaders sermonized on an end to evil, China rose at our expense; our military expeditions in the Middle East ended in frustration, when not failure; and we lost our military edge and many of our economic advantages. But such policies would be even more extraordinarily ill-advised when we are now locked in a strategic rivalry with a superpower China that is far more powerful than the USSR, Germany, or Japan ever were. We simply do not have the preponderance of power to waste our resources anymore.

Time, then, to focus on the region and the contest that really matters: the effort to deny China’s dominance of Asia. We are already well behind in that struggle, and every day we neglect to increase our focus further increases the chances of crisis, war, and defeat—with grievous consequences for all Americans.

#### Strengthening allied power to counter China is the only way to prevent great power war — accommodation makes it inevitable.

Beckley 22 — Michael Beckley, Associate Professor of Political Science at Tufts University, Nonresident Senior Fellow at the American Enterprise Institute, former Senior China Policy Analyst at the Science Applications International Corporation—a government services and IT support company, former Faculty Fellow in National Security in the Office of the Secretary of Defense for Policy Planning at the U.S. Department of Defense, holds a Ph.D. in Political Science from Columbia University, former policy debater at College Prep and Emory University, 2022 (“Enemies of My Enemy: How Fear of China Is Forging a New World Order,” *Foreign Affairs*, March/April, Available Online at https://www.foreignaffairs.com/articles/2021-02-14/china-new-world-order-enemies-my-enemy, Accessed 07-07-2022)

The Clash of Systems

The history of international order building is one of savage competition between clashing systems, not of harmonious cooperation. In the best of times, that competition took the form of a cold war, with each side jockeying for advantage and probing each other with every measure short of military force. In many cases, however, the competition eventually boiled over into a shooting war and ended with one side crushing the other. The victorious order then ruled until it was destroyed by a new competitor—or until it simply crumbled without an external threat to hold it together.

Today, a growing number of policymakers and pundits are calling for a new concert of powers to sort out the world’s problems and divide the globe into spheres of influence. But the idea of an inclusive order in which no one power’s vision prevails is a fantasy that can exist only in the imaginations of world-government idealists and academic theorists. There are only two orders under construction right now—a Chinese-led one and a U.S.-led one—and the contest between the two is rapidly becoming a clash between autocracy and democracy, as both countries define themselves against each other and try to infuse their respective coalitions with ideological purpose. China is positioning itself as the world’s defender of hierarchy and tradition against a decadent and disorderly West; the United States is belatedly summoning a new alliance to check Chinese power and make the world safe for democracy.

This clash of systems will define the twenty-first century and divide the world. China will view the emerging democratic order as a containment strategy designed to strangle its economy and topple its regime. In response, it will seek to protect itself by asserting greater military control over its vital sea-lanes, carving out exclusive economic zones for its firms, and propping up autocratic allies as it sows chaos in democracies. The upsurge of Chinese repression and aggression, in turn, will further impel the United States and its allies to shun Beijing and build a democratic order. For a tiny glimpse of what this vicious cycle might look like, consider what happened in March 2021, when Canada, the United Kingdom, the United States, and the EU sanctioned four Chinese officials for human rights abuses in Xinjiang. The sanctions amounted to a slap on the wrist, but Beijing interpreted them as an assault on its sovereignty and unleashed a diplomatic tirade and a slew of economic sanctions. The EU returned fire by freezing its proposed EU-China Comprehensive Agreement on Investment.

In the coming years, the trade and technology wars between China and the United States that began during the Trump administration will rage on as both sides try to expand their respective spheres. Other countries will find it increasingly difficult to hedge their bets by maintaining links to both blocs. Instead, China and the United States will push their partners to pick sides, compelling them to reroute their supply chains and adopt wholesale the ecosystem of technologies and standards of one side’s order. The Internet will be split in two. When people journey from one order to the other—if they can even get a visa—they will enter a different digital realm. Their phones won’t work, nor will their favorite websites, their email accounts, or their precious social media apps. Political warfare between the two systems will intensify, as each tries to undermine the domestic legitimacy and international appeal of its competitor. East Asian sea-lanes will grow clogged with warships, and rival forces will experience frequent close encounters.

The standoff will end only when one side defeats or exhausts the other. As of now, the smart money is on the U.S. side, which has far more wealth and military assets than China does and better prospects for future growth. By the early 2030s, Xi, an obese smoker with a stressful job, will be in his 80s, if he is still alive. China’s demographic crisis will be kicking into high gear, with the country projected to lose roughly 70 million working-age adults and gain 130 million senior citizens between now and then. Hundreds of billions of dollars in overseas Chinese loans will be due, and many of China’s foreign partners won’t be able to pay them back. It is hard to see how a country facing so many challenges could long sustain its own international order, especially in the face of determined opposition from the world’s wealthiest countries.

Yet it is also far from guaranteed that the U.S.-led democratic order will hold together. The United States could suffer a constitutional crisis in the 2024 presidential election and collapse into civil strife. Even if that doesn’t happen, the United States and its allies might be rent by their own divides. The democratic world is suffering its greatest crisis of confidence and unity since the 1930s. Nationalism, populism, and opposition to globalism are rising, making collective action difficult. The East Asian democracies have ongoing territorial disputes with one another. Many Europeans view China as more of an economic opportunity than a strategic threat and seriously doubt the United States’ reliability as an ally, having endured four years of tariffs and scorn from President Donald Trump, who could soon be back in power. Europeans also hold different views from Americans on data security and privacy, and European governments fear U.S. technology dominance almost as much as they do Chinese digital hegemony. India may not be ready to abandon its traditional policy of nonalignment and back a democratic order, especially when it is becoming more repressive at home, and an order built around democracy will struggle to form productive partnerships with autocracies that would be important partners in any alliance against China, such as Singapore and Vietnam. Fear of China is a powerful force, but it might not be potent enough to paper over the many cracks that exist within the emerging anti-Chinese coalition.

If that coalition fails to solidify its international order, then the world will steadily slide back into anarchy, a struggle among rogue powers and regional blocs in which the strong do what they can and the weak suffer what they must. Some scholars assume—or hope—that an unordered world will sort itself out on its own, that great powers will carve out stable spheres of influence and avoid conflict or that the spread of international commerce and enlightened ideas will naturally maintain global peace and prosperity. But peace and prosperity are unnatural. When achieved, they are the result of sustained cooperation among great powers—that is, of an international order.

Doubling Down On Democracy

History shows that eras of fluid multipolarity typically end in disaster, regardless of the bright ideas or advanced technologies circulating at the time. The late eighteenth century witnessed the pinnacle of the Enlightenment in Europe, before the continent descended into the hell of the Napoleonic Wars. At the start of the twentieth century, the world’s sharpest minds predicted an end to great-power conflict as railways, telegraph cables, and steamships linked countries closer together. The worst war in history up to that point quickly followed. The sad and paradoxical reality is that international orders are vital to avert chaos, yet they typically emerge only during periods of great-power rivalry. Competing with China will be fraught with risk for the United States and its allies, but it might be the only way to avoid even greater dangers.

To build a better future, the United States and its allies will need to take a more enlightened view of their interests than they did even during the Cold War. Back then, their economic interests dovetailed nicely with their geopolitical interests. Simple greed, if nothing else, could compel capitalist states to band together to protect private property against a communist onslaught. Now, however, the choice is not so simple, because standing up to China will entail significant economic costs, especially in the short term. Those costs might pale in comparison to the long-term costs of business as usual with Beijing—Chinese espionage has been estimated to deprive the United States alone of somewhere between $200 billion and $600 billion annually—to say nothing of the moral quandaries and geopolitical risks of cooperating with a brutal totalitarian regime with revanchist ambitions. Yet the ability to make such an enlightened calculation in favor of confronting China may be beyond the capacities of any nation, especially ones as polarized as the United States and many of its democratic allies.

If there is any hope, it lies in a renewed commitment to democratic values. The United States and its allies share a common aspiration for an international order based on democratic principles and enshrined in international agreements and laws. The core of such an order is being forged in the crucible of competition with China and could be built out into the most enlightened order the world has ever seen—a genuine free world. But to get there, the United States and its allies will have to embrace competition with China and march forward together through another long twilight struggle.

#### Nuclear escalation is likely — urgently strengthening allied coordination to send a signal of resolve is the only way to prevent it.

Pettyjohn and Wasser 22 — Stacie L. Pettyjohn, Senior Fellow and Director of the Defense Program at the Center for a New American Security, Adjunct Professor in the School of Advanced International Studies at Johns Hopkins University, former Senior Political Scientist and Director of the Strategy and Doctrine Program of Project AIR FORCE at the RAND Corporation, holds a Ph.D. in Foreign Affairs from the University of Virginia, and Becca Wasser, Fellow in the Defense Program and Co-Leader of The Gaming Lab at the Center for a New American Security, Adjunct Instructor in the School of Foreign Service at Georgetown University, former Senior Policy Analyst at the RAND Corporation, former Program Officer and Research Analyst at the International Institute for Strategic Studies (UK), holds an M.S. in Foreign Service from Georgetown University, 2022 (“A Fight Over Taiwan Could Go Nuclear: War-Gaming Reveals How a U.S.-Chinese Conflict Might Escalate,” *Foreign Affairs*, May 20th, Available Online at https://www.foreignaffairs.com/articles/china/2022-05-20/fight-over-taiwan-could-go-nuclear, Accessed 07-12-2022)

Russia’s invasion of Ukraine has raised the specter of nuclear war, as Russian President Vladimir Putin has placed his nuclear forces at an elevated state of alert and has warned that any effort by outside parties to interfere in the war would result in “consequences you have never seen.” Such saber-rattling has understandably made headlines and drawn notice in Washington. But if China attempted to forcibly invade Taiwan and the United States came to Taipei’s aid, the threat of escalation could outstrip even the current nerve-wracking situation in Europe.

A recent war game, conducted by the Center for a New American Security in conjunction with the NBC program “Meet the Press,” demonstrated just how quickly such a conflict could escalate. The game posited a fictional crisis set in 2027, with the aim of examining how the United States and China might act under a certain set of conditions. The game demonstrated that China’s military modernization and expansion of its nuclear arsenal—not to mention the importance Beijing places on unification with Taiwan—mean that, in the real world, a fight between China and the United States could very well go nuclear.

Beijing views Taiwan as a breakaway republic. If the Chinese Communist Party decides to invade the island, its leaders may not be able to accept failure without seriously harming the regime’s legitimacy. Thus, the CCP might be willing to take significant risks to ensure that the conflict ends on terms that it finds acceptable. That would mean convincing the United States and its allies that the costs of defending Taiwan are so high that it is not worth contesting the invasion. While China has several ways to achieve that goal, from Beijing’s perspective, using nuclear weapons may be the most effective means to keep the United States out of the conflict.

Gearing For Battle

China is several decades into transforming its People’s Liberation Army (PLA) into what the Chinese President Xi Jinping has called a “world-class military” that could defeat any third party that comes to Taiwan’s defense. China’s warfighting strategy, known as “anti-access/area denial,” rests on being able to project conventional military power out several thousand miles in order to prevent the American military, in particular, from effectively countering a Chinese attack on Taiwan. Meanwhile, a growing nuclear arsenal provides Beijing with coercive leverage as well as potentially new warfighting capabilities, which could increase the risks of war and escalation.

China has historically possessed only a few hundred ground-based nuclear weapons. But last year, nuclear scholars at the James Martin Center for Nonproliferation Studies and the Federation of American Scientists identified three missile silo fields under construction in the Xinjiang region. The Financial Times reported that China might have carried out tests of hypersonic gliders as a part of an orbital bombardment system that could evade missile defenses and deliver nuclear weapons to targets in the continental United States. The U.S. Department of Defense projects that by 2030, China will have around 1,000 deliverable warheads—more than triple the number it currently possesses. Based on these projections, Chinese leaders may believe that as early as five years from now the PLA will have made enough conventional and nuclear gains that it could fight and win a war to unify with Taiwan.

Our recent war game—in which members of Congress, former government officials, and subject matter experts assumed the roles of senior national security decision makers in China and the United States—illustrated that a U.S.-Chinese war could escalate quickly. For one thing, it showed that both countries would face operational incentives to strike military forces on the other’s territory. In the game, such strikes were intended to be calibrated to avoid escalation; both sides tried to walk a fine line by attacking only military targets. But such attacks crossed red lines for both countries, and produced a tit-for-tat cycle of attacks that broadened the scope and intensity of the conflict.

For instance, in the simulation, China launched a preemptive attack against key U.S. bases in the Indo-Pacific region. The attacks targeted Guam, in particular, because it is a forward operating base critical to U.S. military operations in Asia, and because since it is a territory, and not a U.S. state, the Chinese team viewed striking it as less escalatory than attacking other possible targets. In response, the United States targeted Chinese military ships in ports and surrounding facilities, but refrained from other attacks on the Chinese mainland. Nevertheless, both sides perceived these strikes as attacks on their home territory, crossing an important threshold. Instead of mirror-imaging their own concerns about attacks on their territory, each side justified the initial blows as military necessities that were limited in nature and would be seen by the other as such. Responses to the initial strikes only escalated things further as the U.S. team responded to China’s moves by hitting targets in mainland China, and the Chinese team responded to Washington’s strikes by attacking sites in Hawaii.

A New Era

One particularly alarming finding from the war game is that China found it necessary to threaten to go nuclear from the start in order to ward off outside support for Taiwan. This threat was repeated throughout the game, particularly after mainland China had been attacked. At times, efforts to erode Washington’s will so that it would back down from the fight received greater attention by the China team than the invasion of Taiwan itself. But China had difficulty convincing the United States that its nuclear threats were credible. In real life, China’s significant and recent changes to its nuclear posture and readiness may impact other nations’ views, as its nuclear threats may not be viewed as credible given its stated doctrine of no first use, its smaller but burgeoning nuclear arsenal, and lack of experience making nuclear threats. This may push China to preemptively detonate a nuclear weapon to reinforce the credibility of its warning.

China might also resort to a demonstration of its nuclear might because of constraints on its long-range conventional strike capabilities. Five years from now, the PLA still will have a very limited ability to launch conventional attacks beyond locations in the “second island chain” in the Pacific; namely, Guam and Palau. Unable to strike the U.S. homeland with conventional weapons, China would struggle to impose costs on the American people. Up until a certain point in the game, the U.S. team felt its larger nuclear arsenal was sufficient to deter escalation and did not fully appreciate the seriousness of China’s threats. As a result, China felt it needed to escalate significantly to send a message that the U.S. homeland could be at risk if Washington did not back down. Despite China’s stated “no-first use” nuclear policy, the war game resulted in Beijing detonating a nuclear weapon off the coast of Hawaii as a demonstration. The attack caused relatively little destruction, as the electromagnetic pulse only damaged the electronics of ships in the immediate vicinity but did not directly impact the U.S. state. The war game ended before the U.S. team could respond, but it is likely that the first use of a nuclear weapon since World War II would have provoked a response.

The most likely paths to nuclear escalation in a fight between the United States and China are different from those that were most likely during the Cold War. The Soviet Union and the United States feared a massive, bolt-from-the-blue nuclear attack, which would precipitate a full-scale strategic exchange. In a confrontation over Taiwan, however, Beijing could employ nuclear weapons in a more limited way to signal resolve or to improve its chances of winning on the battlefield. It is unclear how a war would proceed after that kind of limited nuclear use and whether the United States could de-escalate the situation while still achieving its objectives.

An Ounce of Prevention

The clear lesson from the war game is that the United States needs to strengthen its conventional capabilities in the Indo-Pacific to ensure that China never views an invasion of Taiwan as a prudent tactical move. To do so, the United States will need to commit to maintaining its conventional military superiority by expanding its stockpiles of long-range munitions and investing in undersea capabilities. Washington must also be able to conduct offensive operations inside the first and second island chains even while under attack. This will require access to new bases to distribute U.S. forces, enhance their survivability, and ensure that they can effectively defend Taiwan in the face of China’s attacks.

Moreover, the United States needs to develop an integrated network of partners willing to contribute to Taiwan’s defense. Allies are an asymmetric advantage: the United States has them, and China does not. The United States should deepen strategic and operational planning with key partners to send a strong signal of resolve to China. As part of these planning efforts, the United States and its allies will need to develop war-winning military strategies that do not cross Chinese red-lines. The game highlighted just how difficult this task may be; what it did not highlight is the complexity of developing military strategies that integrate the strategic objectives and military capacities of multiple nations.

Moving forward, military planners in the United States and in Washington’s allies and partners must grapple with the fact that, in a conflict over Taiwan, China would consider all conventional and nuclear options to be on the table. And the United States is running out of time to strengthen deterrence and keep China from believing an invasion of Taiwan could be successful. The biggest risk is that Washington and its friends choose not to seize the moment and act: a year or two from now, it might already be too late.

## 1AC (Less Highlighted)

### 1AC — RMA Advantage

#### Contention One: RMA

#### Emerging and disruptive technology (EDT) is creating a new Revolution in Military Affairs (RMA), but NATO has been slow to adapt — this will decimate its technological superiority.

Havránek and Bagge 21 — Jan Havránek, Deputy Minister of Defense of the Czech Republic, former Policy Adviser at the Policy Planning Unit at the Office of the NATO Secretary General, holds an M.A. in International Relations from Tufts University, and Daniel P. Bagge, Independent Specialist in Emerging and Disruptive Technology, former Cyber Attaché of the Czech Republic to the United States, former Director of Cyber Security Policies in the National Cyber and Information Security of the Czech Republic, former Member of the Cyber Security Strategy Expert Group at the European Union, holds an M.A. in International Relations and National Security Studies from the George C. Marshall European Center for Security Studies (Germany) and Bundeswehr University Munich (Germany), 2021 (“Technology Adoption: Are we too late to the party?,” *Small Wars Journal*, July 18th, Available Online at https://smallwarsjournal.com/jrnl/art/technology-adoption-are-we-too-late-party, Accessed 07-12-2022)

Introduction

NATO and the West are experiencing a reversed kind of revolution in military affairs (RMA) with new technologies bearing far-reaching implications beyond the conduct of war. Past revolutions in military spilled from the battlefield to the civilian sector. They had an effect either by directly impacting the result of a given conflict or through adoption of military technical advantages in non-military aspects of life. Today, we see an opposite trend brought by the private and non-military, non-governmental actors. In their everyday lives, general publics and governments alike face military-grade technologies developed and applied by the commercial sector. And it is the private sector that enjoys exclusivity over these technologies while the military lags behind.

How information is gathered, processed, analysed, communicated, distributed, and utilized has always underlined military planning and assumptions for success in conflict. For example, the reconnaissance strike complex introduced by the Soviets was based on real-time intelligence gathering and underpinned by automated systems and fast data processing. Similarly, NATO’s deep attack concept assumed that commanders “would be given the automated assessment means necessary to rapidly analyse the enemy’s force array.”[1] Such concepts, however innovative and tech-based, assumed a relatively limited amount of data and relied heavily on the human factor. Today, in the era of cloud computing and artificial intelligence, there is a clear shift towards sensor-centric, automated processing. Reconnaissance and analysis are becoming as important as firepower and kinetic effects. Humans are being pushed out from the decision-making due to the quantity of information gathered/coming from the battlefield. The hyper-speed warfare (or the “hyper war,” a term linking the intensity of conflict with cybernetics) risks making the human factor almost obsolete. To a certain extent, human presence in the loop will consequently become more a question of morality and less of efficacy.

None of this is science fiction, as modern technologies enabling hyper war already exist. The question for NATO and the West is not whether they choose to adopt these technologies but how they should adopt them to their benefit.

The situation is even more complicated if we consider the myriad of actors involved in international security. In the past, timing and accuracy of decision-making depended on a system designed by the state, was utilized on the state level, and made for the state’s purpose. Today, external entities such as corporations, non-state actors, groups of citizens and individuals matter as well. They hold the power and the technological means to exercise significant pressure over state affairs. Some even have the ability to largely cripple the functioning of governments and state services.

This development poses a significant challenge to NATO’s ability to deliver on its core tasks. If the Alliance wants to successfully continue its political-military adaptation, it will need a new approach to decision-making, operational planning, and crisis management.

This article addresses some of the key issues the Alliance needs to consider as it navigates through the new kind of revolution in military affairs: 1) the changing character of warfare; 2) the domination of the private sector over the military in the deployment of commercial technology with military potential; 3) and the interdependence of decision-making and modern technology.

The Changed Nature of Warfare

Modern technologies are changing the nature of warfare, as they have throughout the human history. In many instances, introduction of new weaponry constituted for a tactical advantage on the battlefield, occasionally reaching a strategic-level impact. An example of that can be the introduction of the British longbow at the Battle of Agincourt. Other technologies changed profoundly how militaries operate and wage war. Among such examples are railroads, telegraph, radar, combustion engine, jet engine, or radio frequencies-based communication equipment. The revolutionary nature of these technologies usually brings about significant changes in defence planning, command and control, and force organization.

For any institution, be it a nation state, a large bureaucracy, or an international alliance such as NATO, the ability to adopt disruptive technologies is key. The adoption usually leads to a larger structural adaptation: The use of standardized calibres in the French Revolutionary and Napoleonic Wars allowed for greater flexibility and uniformity of the French forces. The first use of Marconi’s wireless telegraphy by the British armed forces in the Anglo-Boer War (1899-1902) changed the way how military communicated. The use of railroads in the 19th century wars had a strategic effect on the mobility and supply of forces. Finally, the deployment of radar technology during World War 2 improved both defensive and offensive capacities of the militaries, and, as a result, probably saved thousands of lives. In all these instances, the military advancement of technologies spilled over to the civilian side as well.

In the past five decades, military science theorists have been dealing with the evolution in warfare in more detail. Although the main focus was dedicated to the then-ongoing Cold War, scholars from the field made a number of predictions that have proven to be correct. They correctly understood that technological advancement was gaining momentum and that the upcoming changes were not going be evolutionary but would come in leaps.[2]

Three concepts also emerged from this thinking: military technical revolution (MTR), revolution in military affairs (RMA), and military revolution (MR). Even though they stand individually, all three concepts are closely interconnected. For example, technology or a weapon platform that has reached the level of military technical revolution can, in the end, reach the level of military revolution as long as it constitutes considerable changes to organizational structure and operational art. In several cases, the MTR, RMA and MR are seen as one concept altogether.[3]

Military Technical Revolution, Revolution in Military Affairs, and Military Revolution

An event has to meet several conditions to qualify as a MTR/RMA/MR. A revolution is defined by a profound change in military systems, operational art, and organizational adjustment. Simple introduction of new technology or military platform does not constitute an MTR.

As Andrew F. Krepinevich, a defence policy analyst, writes,[4] a real-world example of military technical revolution can be unmanned combat vehicles and their role in conducting combat and ISR operations. Another example are cyber defence/offense oriented forces that fulfil the following criteria: technological change—introduction of new military platforms; evolution of military systems; operational innovation (e.g., cyberspace defence planning); or organizational adaptation impacting force structure and organizational units.

A military revolution in effect alters the way in which power is projected. Apart from changing the shape and form of warfare, it spills over from the military organizational structures and battlefields into societal, economic, and political domains.

The above-mentioned enablers of military revolution, such as artificial intelligence and quantum technology applications, show promising potential in changing the current societal fabric and effectively impacting societal, political, and military affairs.

Among the decisive factors, universal to all combat operations, is time. As the pace of technological advancement increases, the potential effects of a technology are no longer the most important factor. Equally important is the pace of adaption: how fast a technology can be utilized and how it recalibrates the relation between action and reaction. As time remains of immense importance, the ability to share information and move forces around based on that information can be the decisive factor in conflict. The speed of information sharing can thus be considered a military revolution.[5] The introduction of combustion engines and the changes it brought to operational art, manoeuvring, and transport of forces, changed the time factor. Unparalleled sensory awareness, communication, and automation have the same potential.

Consequently, time available for decision-making will continue to shrink. Decision makers will have to be equipped with information and intelligence as accurate as possible. The “speed of information” will be critical to provide political guidance to commanders or even to conduct a pre-emptive strike. There may be instances when the pace of combat operations will increase to a threshold where defensive action will be rendered useless.[6] Technology that can process this “speed of information” will affect the entire decision-making algorithm and broader perception of security and defence in society.

Militarization of Technology and the Role of Private Sector

The 21st century introduced an unparalleled speed of innovation and dissemination of (digital) technology among the general population and the private sector. It also hindered states’ ability to remain the sole proprietor of military grade applications. This is due to an unprecedented redistribution of applied research from the government level towards the private sector. Today, private entities commercialize disruptive technologies and provide them directly to the customers, unleashing military level applications into the wild. The governments, namely national security and defence domains are lagging behind in adoption of innovative technologies. This is evident from the spending on military research and development, which is dim in comparison to its private sector equivalents.[7] For example, in 2004, the global spending on civilian research and development was approximately ten times as large as global military research and development.[8]

Emerging disruptive technologies are thus becoming more accessible. The interdependency between state instruments of power (including armed forces) and civilian technology is growing and is expected to grow even further. In the past, military platforms were developed by the private sector, but their sole purpose was defined by the military. Today’s world brings the challenge of dual-use technology that is researched, manufactured, and provided entirely by the private sector, while having military application. Which effectively impacts the competitiveness on the battlefield. With facial recognition, targeting, and other artificial intelligence-powered applications (including micro targeting on social networks), the interest of the private sector and state actors overlap and are often blurred. It is common for state actors to be dependent on private sector providers. Sometimes to the extent where the government is unable to adjust the technologies’ conditions for its purposes, as the usual customer base lies in the civilian business world.

The rise of corporations and digital tycoons brought about democratization of technologies and their global spread in an unprecedented speed, resulting in a digital interdependency. States have been replaced by private entities who hold the keys to information flow and disruptive technologies. These technologies are often introduced to the general public sooner than the governmental bodies even have a chance to understand them.

Technological superiority has always played a significant role in international relations. It usually derived from the use of force and was traditionally in the hands of the state. In the past few decades, non-state entities started surpassing the state’s control. Technology provided by corporations paired with ideology and strategic interests of various state actors. However, state actors were not equipped with proper organizational structures and decision-making processes to stay up to date. As result, they have been left behind not to lead, but to react to technological progress and innovations.

Quantum research on sensors[9] can be an example of the private sector’s success. Non-state actors currently both employ the leading scientists in the field and conduct research in cooperation with competing state interests. All that despite the efforts of the governmental bodies and the military to fund innovative research.[10] This substantially increases the prospects of quantum related applications being provided to the general population before they are utilized by the military, leading to a loss in competitiveness on the battlefield.

The issue is caused by the inability of governmental entities to appreciate the need to conduct basic and applied research competitively with the private sector. In order for it to be done correctly, it would require a substantial organizational change and the ability to understand the potential impacts of disruptive technologies. That is also necessary for proper resource allocation. Modern and disruptive technologies are part of the non-conventional military risks and destabilizing efforts that governmental structures fail to address. A number of technological platforms, social networks, and digital enablers have become tools of digital deceit. They have been used to target the general population, which was unaware of being exposed to hybrid tactics and military grade influence operations.[11] This was enabled by overlaps of influence-operation techniques from the military field into the private sector. Private companies also applied these techniques in target group advertising.

This is not the first time the West has had to deal with ideological competitors trying to gain supremacy. The Cold War was about both ideology and technology, with the stark example of Operation Farewell.[12] Even then, technological superiority was meant to promote ideological and strategic interests. The combination of ideology and technology continued to be a factor in the post-Cold War world. An example of that can be terrorist organizations and their use of basic available technology. The situation in 2021 is, however, starkly different from the 1980’s or the 2000s for a number of reasons:

\* As argued earlier, the character of warfare has changed profoundly; technologically driven warfare has entered the soft power arena.

\* The pace of military operations and general interactions has increased— he human capacity is now limited not only by the speed of events but also by the amount of information collected, processed, and analysed from the battlefield. The ISR platforms are collecting so much data and raw intelligence that it is necessary to automate processes previously not constrained by human capacity or reaction speed demands. The changes pushing the limits of human operators and analysts happen in leaps and are fast paced.

\* What is more: private sector capacities play a significant role in international power competition. Technological tycoons represent stand-alone actors risen on the wealth and influence of the technology they provide. They have also become the tools of state influence. Understanding this shift is hard, as we tend to differentiate between private entities, corporations with presence on the global markets, and state actors. However, in many cases, the private corporations are bound by national legislation, hiding as agents of influence in plain sight.

\* As a result, we see traditional technological powers (the West, led by the United States, with Europe lagging behind) and democratic tech tycoons, including Japan, South Korea, and Taiwan, capitalizing on the asymmetry provided by modern technologies. While China, Russia, and India aspire to supersede them, this aspiration is evident from both their official policies and their investment in new technologies and defence modernization. What started as mainly intellectual property transfer and theft[13] has now turned into a full-fledged technological adoption race.[14]

Implications for NATO

So where does all this leave NATO? In 2021, as NATO has already begun to define its vision for the next ten years, it faces three principle challenges:

1. Ensuring that decision-makers understand the sheer potential derived from emerging and disruptive technologies and how they will impact the Alliance’s governance and decision models.

2. Prioritizing what technologies, the Alliance should pursue, when, and how they fit into NATO’s wider posture;

3. Sharing the technological burden equally across the Alliance.

Raising awareness among political leaders about the new technologies’ impact on NATO may not be as simple as it seems. Currently, there is a growing gap in perception of the new technology’s importance between the political and military level. Military authorities of the Alliance have, for a long time, been highlighting the need for innovation and adoption of new technologies.[15] Trials of innovative technological solutions and new capabilities have been part of NATO’s military training and exercises. For example, NATO now regularly tests unmanned systems in the maritime area[16] and there is work being done in the area of Electronic Spectrum warfare. Furthermore, adoption of new technologies in new capabilities development has been encouraged through the NATO Defence Planning Process (NDPP). In 2018, the Allied Command Transformation developed Emerging and Disruptive Technologies Roadmap, which received political endorsement at the meeting of defence ministers in June 2019.

On the political front, the effort has been slower. Until recently, the Allies themselves have maintained a rather declaratory approach to technology and innovation. Later, in 2020, the Secretary General appointed an innovation advisory group to provide counsel on NATO’s next steps in the tech area. A full political strategy on the emerging and disruptive technologies was finally adopted at the Brussels Summit in June 2021: “[T]his strategy seeks to preserve our interoperability; safeguard our sensitive technologies; and actively address the threats and challenges posed by technological developments by others, both now and in the future. Drawing on the extensive innovation expertise of all 30 Allies, we will further leverage our partnerships, including with the private sector and academia, to maintain our technological edge.[17]”

The Allies pledged to launch a civil-military Defence Innovation Accelerator for the North Atlantic (DIANA) and to establish a NATO Innovation Fund. The aim is to promote interoperability, foster development and adoption of technological solutions, and to allow individual NATO Members to support start-ups working on dual use emerging and disruptive technologies relevant to NATO’s security. The Allies also agreed to continue developing capabilities in the technological domain and recognized the need for research and development and innovation to meet the challenges emerging and disruptive technologies pose. Some of the specific areas where new capabilities must be acquired are air-to-air refuelling, training, precision strike, munitions, air defence, CBRN defence, autonomous systems, and next-generation rotorcraft capability.[18]

The process will require effective prioritization. The afore-mentioned NATO Defence Planning Process already accounts for future technological change in military capability development. Allies have a free reign in how they wish to meet the target, including what platform and technology they wish to choose. The pitfall of this approach lies in the traditional view of military technology adoption and capability development. More specifically, the issue is the government-centric model that operates with significantly longer lifecycles as well as the ownership structures that find no applicable parallel in the private sector’s current pacing and push out of emerging and disruptive technologies.

It will be up to NATO to use both its new and already-existing tools to help navigate through these technologies and decide on which to adopt first. Together with the Allies and the private sector, NATO/DIANA should scan the horizon and say which new technologies are to be integrated with highest priority. NATO must then proceed with the integration into its planning (both capability and civil emergency), training and exercises, as well as the Alliance’s wider consultation and decision-making.

The adoption must happen systematically, at the highest political level. The Brussels Summit should be an impulse for the Council to start incorporating more technologically driven discussions into its deliberations. Scenario-based discussions and NATO’s high-level exercise program should include situations where emerging and disruptive technologies play a decisive role. None of this requires any radical changes to the decision-making procedures or new tools.

Although the NATO Innovation Fund is a step in the right direction, it must reflect the disparities that exist among individual Member States in this context. Many Allies have national assets that fulfil various tech innovation functions. For example, the UK’s jHub Defence Innovation helps integrate market-ready solutions into military.[19] In 2020, Germany established an agency for innovation in cyber security to promote technological innovation and solutions that would enhance the country’s security.[20] NATO should serve as a platform where nations with more advanced structures, know-how and capabilities come forward and share some of these solutions and findings with other Allies.

The NATO Innovation Fund should also facilitate burden-sharing in this area. Emerging and disruptive technologies have so far been guarded as a national treasure; their application and availability in multinational context has been scarce. In the future, not all Allies will possess or have access to new technologies shaping the military capabilities and conduct. Some countries will be faster in technological adoption. Others may not be able to afford new technologies, if they are to meet all other requirements for NATO’s collective defence. The Fund can be a mechanism that balances out these gaps and spreads the burden more equally among the Allies. NATO must now design a system of allocation—currently envisioned on a voluntary basis—that will motivate the Allies to contribute to it. This must take into account national requirements that might be limiting for some Allies and the danger of duplicity with similar endeavours.

There are several examples of sharing mechanisms that NATO has successfully adopted in the past and can now build on: 1) Nuclear-sharing arrangements where non-nuclear members of NATO support potential nuclear missions and the decision-making without possessing the nuclear technology; 2) Common-funded capability models, such as the Allied Ground Surveillance system or NATO’s Ballistic Missile Defence, where Allies fund and outsource the development of technology through common / joint financial contributions; while both slightly different in structure and funding, both are an example of technology funded by some Allies, but made available to the entire Alliance. Both examples link to previous revolutions in military affairs. Until now, the closest the Allies have come to having a new technology sharing mechanism is the Sovereign Cyber Effects Provided Voluntarily by Allies mechanism. It allows the Supreme Allied Commander Europe (SACEUR) to request offensive effects to be delivered on a designated target, without sharing the technology with others.[21]

All these examples have one thing in common: technological know-how and intellectual property remains in the hands of the capability providers. This gives NATO an opportunity to forge new tech-sharing arrangements that would include individual Allies and the private sector. This could also prevent the technological gap among Allies from widening any further.

One specific solution could be creating a private sector parallel to NATO’s political partnerships. However, the criteria for such partnerships might be hard to agree on. NATO would have to find a way to satisfy some highly political questions, such as: What companies and what technologies would be represented? Or would Allies even be able and willing to generate funds to support a NATO-branded research & development?

In the meantime, NATO must approach the prioritization of emerging and disruptive technologies by employing its traditional strengths: define its technological requirements through the prism of military requirements and forge a consensus among thirty Allies on the general technological pathway. When NATO sets the standards, individual Allies are usually very capable of delivering, according to their national preferences and legislation.

Lastly, in its ongoing efforts to address the challenge of emerging and disruptive technologies, NATO must take into account similar, already existing or maturing projects and structures. The European Union sees emerging and disruptive technologies as a crucial issue and has developed mechanisms through which they are tackled. The European Defence Agency recognizes technological development as one of the main pillars of its work and provides a useful platform for international cooperation. It aims to support Member States in developing and improving capabilities on a cutting-edge technological level of its Member States and shape their national strategies in this area. The European Defence Fund deals with both technological research and defence capability development and even specifically allocates a part of its financial resources for disruptive technologies.

A major task for the two organizations will now be to find a way to cooperate on this issue and avoid undesirable duplication. The Alliance and the EU must come up with a solution where the EuroAtlantic area is capable of adapting to the ever-changing security environment and can readily adopt fast-advancing technologies. What is more, both sides of the Atlantic must be equally capable partners in this cooperation and burden sharing.

Conclusion

Technological change is real, fast paced, and greatly affects NATO’s civilian-military structures. Never has the Alliance faced so many technological changes that would reach beyond the traditional realm of security and defence.

In the 1990s, the key political question for the future of NATO was whether to adapt by going out of area (in terms of operations and membership) or go out of business. The question for the next couple of years is essentially the same; it touches the very purpose and existence of the Alliance and the utility of NATO: How to make sure that NATO stays technologically relevant so that it can maintain its function and capabilities. Complacency and general political statements will not suffice. The private sector, which is the principal agent of the new kind of revolution in military affairs, is technologically advancing in leaps. If NATO is not able to keep up with this change in organization of geopolitics and technology, it will have to change its organizational structure. With modern and disruptive technologies becoming more mainstream and moving into wider governance structures, similar adjustments will be necessary in NATO’s daily business operations.

NATO can successfully navigate the new wave of revolution in military affairs; however, it must first change its political culture and overall approach to modern and disruptive technologies. It also needs to develop new technology-sharing mechanisms that will be fair to all Allies. There may be different approaches to this change: a reform of NATO’s procurement agencies, a reform of financial mechanisms, or a partnership reform. Either way, any such effort will have to build on the active participation of the private sector. Only then will NATO be able to maintain its technological edge in the future.

#### Failing to maintain NATO’s technological superiority will cause great power nuclear war — out-competing Russia and China in the EDT RMA is key.

Kroenig 21 — Matthew Kroenig, Professor in the Department of Government and the Edmund A. Walsh School of Foreign Service at Georgetown University, Director of the Global Strategy Initiative and Deputy Director of the Scowcroft Center for Strategy and Security at the Atlantic Council, former Special Government Employee and Senior Policy Adviser to the Office of the Assistant Secretary of Defense for Strategy, Plans, and Capability/Nuclear and Missile Defense Policy at the U.S. Department of Defense, former Stanton Nuclear Security Fellow at the Council on Foreign Relations, holds a Ph.D. in Political Science from the University of California-Berkeley, 2021 (“Will Emerging Technology Cause Nuclear War?: Bringing Geopolitics Back In,” *Strategic Studies Quarterly*, Volume 15, Issue 4, Winter, Available Online to Subscribing Institutions via EBSCO Open Access Journals, p. 64-70)

***[\*\*\* Note: 4IR*** *= “The world is experiencing a fourth industrial revolution (4IR) in which a wave of new and transformative technologies is being developed, including artificial intelligence (AI), additive manufacturing, quantum information technology, hypersonic missiles, biotechnology, and directed energy.4 While these technologies are expected to have profound implications for societies and economies, most are dual use and will also affect national security, including nuclear strategic stability.” (p. 59)* ***\*\*\*]***

New Tech Arms Race

Many analysts believe the emerging technology of the 4IR could profoundly affect military capabilities and operational concepts.35 New technology has had revolutionary effects on warfare and international politics throughout history from the Bronze Age to the gunpowder and nuclear revolutions.36

New technologies with direct military application are in development, including AI, quantum information technology, hypersonic missiles, directed energy, additive manufacturing, and biotechnology. How exactly these technologies will affect the future of warfare is still uncertain. The [end page 64] National Defense Strategy Commission report charges that the United States lacks clear operational concepts for combat with Russia and China.37 Still, there is reason to believe these new technologies could have meaningful military applications but perhaps not to the advantage of the United States and its Allies and partners. At present, Russia and especially China might transcend the United States and its Allies and partners in some key 4IR technologies.

Indeed, AI could transform the future of warfare, including through the development of lethal autonomous systems.38 These “killer robots” may lower the threshold of conflict by allowing political leaders to take a country to war without risking the lives of human soldiers. When produced in large numbers, these drones could operate in swarms that overwhelm enemy military platforms and targets.39

Artificial intelligence could also be employed to rapidly sort through vast quantities of data, improving intelligence, surveillance, and reconnaissance and making it easier to track and target enemy forces. The United States retains important advantages in AI, including through its world-leading university system. But China, with its large population and surveillance tactics, has access to more data to train its AI algorithms.40 Beijing is also less constrained by ethical and moral concerns and has the lead in some applications of AI, including facial-recognition technology.

Quantum computing promises information advantages including the ability to have secure, encrypted communications and to decode enemy communications. In its 2021 Military Balance report, the International Institute for Strategic Studies states, “the integration of quantum technologies currently represents one of the most anticipated advances for armed forces. … There is little doubt that they will have disruptive effect when they are employed at scale.”41 China may have the edge in this area, as it was the first country to conduct a successful test of a quantum satellite.42

Space and cyber are increasingly important military domains. Space-based weapons, sensors, defensive interceptors, and the diffusion of counterspace capabilities will make space an increasingly contested military environment.43 The United States is relatively more dependent on space-based assets and computers than its rivals, and the US Department of Defense warns Russia and China will likely employ cyber and counter- space attacks in the early stage of any conflict with the United States in a bid to disrupt US command, control, communications, computers, intel- ligence, surveillance, and reconnaissance (C4ISR).44

Hypersonic missiles, maneuverable and able to travel at over five times the speed of sound, could allow states to conduct low- or no-warning attacks [end page 65] and to evade missile defenses.45 These weapons could also execute large-scale, nonnuclear strategic attacks, the rate of speed compressing the decision-making time leaders have to respond to such attacks. Although the United States developed the initial concepts for these weapons, Russia and China have prioritized their production, testing, and deployment. China has conducted more hypersonic tests than any other nation, and Moscow and Beijing have deployed hypersonic weapons.46

Many other emerging technologies have military applications. Directed-energy microwaves and lasers could allow states to develop more effective integrated air and missile defense systems or to degrade an enemy’s command and control.47 Additive manufacturing could greatly reduce the cost of producing component parts of military platforms and creates the potential for large and rapid quantitative increases in weapons systems, from drones and tanks to submarines and nuclear weapons.48

Biotechnology could be exploited to produce “super soldiers.” China has genetically engineered beagles with three times the muscle mass of a typical canine, a technology that could possibly be applied to humans.49 Exoskeletons could provide soldiers with superhuman strength, and brain implants promise superior cognitive performance. China employed exoskeletons in combat in its 2020 border conflict with India.50

It is not yet clear how these new technologies, when combined with novel operational concepts, will affect the future of warfare, but it is likely they will. A future state may, for example, be able to use additive manufacturing to produce masses of inexpensive drones directed by new AI algorithms to swarm and overwhelm adversaries.51 The attack might be preceded by cyber and counterspace attacks that blind an adversary and disrupt its command and control.

Following a successful advance, the country could then employ directed-energy weapons, autonomous mines, and other advanced defenses to lock in territorial gains and thwart enemy attempts to roll back its aggression. It is possible that the first state to hone these technologies and devise effective operational concepts will have a military edge over its opponents.

Novel Applications

How will states use such a newfound advantage? Technology rarely fundamentally changes the nature or objectives of states. More often, states use technology to advance preexisting geopolitical aims. Moreover, enhanced power can result in greater ambition. Given the geopolitical landscape described, it is likely the United States and its Allies and partners at the core [end page 66] of the international system will behave differently with new military technologies than will revisionist powers, such as Russia and China.

The spread of new technology to the United States and its Allies and partners would likely serve, on balance, to reinforce the existing sources of stability in the prevailing international system. At the end of the Cold War, the United States and its Allies and partners achieved a technological- military advantage over its great power rivals, with the US using its unipolar position to deepen and expand a rules-based system. They also employed their military dominance to counter perceived threats from rogue states and terrorist networks. The United States, its Allies, and partners did not, however, engage in military aggression against great power, nuclear-armed rivals or their allies.

In the future, these status quo powers are apt to use military advantages to reinforce their position in the international system and to deter attacks against Allies and partners in Europe and the Indo-Pacific. These states might also employ military power to deal with threats posed by terrorist networks or by regional revisionist powers such as Iran and North Korea. But it is extremely difficult to imagine scenarios in which Washington or its Allies or partners would use newfound military advantages provided by emerging technology to conduct an armed attack against Russia or China.

Similarly, Moscow and Beijing would likely use any newfound military strength to advance their preexisting geopolitical aims. Given their very different positions in the international system, however, these states are likely to employ new military technologies in ways that are destabilizing. These states have made clear their dissatisfaction with the existing international system and their desire to revise it. Both countries have ongoing border disputes with multiple neighboring countries.

If Moscow developed new military technologies and operational concepts that shifted the balance of power in its favor, it would likely use this advantage to pursue revisionist aims. If Moscow acquired a newfound ability to more easily invade and occupy territory in Eastern Europe, for example (or if Putin believed Russia had such a capability), it is more likely Russia would be tempted to engage in aggression.

Likewise, if China acquired an enhanced ability through new technology to invade and occupy Taiwan or contested islands in the East or South China Seas, Beijing’s leaders might also find this opportunity tempting. If new technology enhances either power’s anti-access, area-denial network, then its leaders may be more confident in their ability to achieve a fait accompli attack against a neighbor and then block a US-led liberation. [end page 67]

These are precisely the types of shifts in the balance of power that can lead to war. As mentioned previously, the predominant scholarly theory on the causes of war—the bargaining model—maintains that imperfect information on the balance of power and the balance of resolve and credible commitment problems result in international conflict.52 New technology can exacerbate these causal mechanisms by increasing uncertainty about, or causing rapid shifts in, the balance of power. Indeed as noted above, new military technology and the development of new operational concepts have shifted the balance of power and resulted in military conflict throughout history.

Some may argue emerging military technology is more likely to result in a new tech arms race than in conflict. This is possible. But Moscow and Beijing may come to believe (correctly or not) that new technology provides them a usable military advantage over the United States and its Allies and partners. In so doing, they may underestimate Washington.

If Moscow or Beijing attacked a vulnerable US Ally or partner in their near abroad, therefore, there would be a risk of major war with the potential for nuclear escalation. The United States has formal treaty commitments with several frontline states as well as an ambiguous defense obligation to Taiwan. If Russia or China were to attack these states, it is likely, or at least possible, that the United States would come to the defense of the victims. While many question the wisdom or credibility of America’s global commitments, it would be difficult for the United States to simply back down. Abandoning a treaty ally could cause fears that America’s global commitments would unravel. Any US president, therefore, would feel great pressure to come to an Ally’s defense and expel Russian or Chinese forces.

Once the United States and Russia or China are at war, there would be a risk of nuclear escalation. As noted previously, experts assess the greatest risk of nuclear war today does not come from a bolt-out-of-the-blue strike but from nuclear escalation in a regional, conventional conflict.53 Russian leaders may believe it is in their interest to use nuclear weapons early in a conflict with the United States and NATO.54 Russia possesses a large and diverse arsenal, including thousands of nonstrategic nuclear weapons, to support this nuclear strategy.

In the 2018 Nuclear Posture Review, Washington indicates it could retaliate against any Russian nuclear “de-escalation” strikes with limited nuclear strikes of its own using low-yield nuclear weapons.55 The purpose of US strategy is to deter Russian strikes. If deterrence fails, however, there is a clear pathway to nuclear war between the United States and Russia. [end page 68] As Henry Kissinger pointed out decades ago, there is no guarantee that, once begun, a limited nuclear war stays limited.56

There are similar risks of nuclear escalation in the event of a US-China conflict. China has traditionally possessed a relaxed nuclear posture with a small “lean and effective” deterrent and a formal “no first use” policy. But China is relying more on its strategic forces. It is projected to double—if not triple or quadruple—the size of its nuclear arsenal in the coming decade.57

Chinese experts have acknowledged there is a narrow range of contingencies in which China might use nuclear weapons first.58 As in the case of Russia, the US Nuclear Posture Review recognizes the possibility of limited Chinese nuclear attacks and also holds out the potential of a limited US reprisal with low-yield nuclear weapons as a deterrent.59 If the nuclear threshold is breached in a conflict between the United States and China, the risk of nuclear exchange is real.

In short, if a coming revolution in military affairs provides a real or perceived battlefield advantage for Russia or China, such a development raises the likelihood of armed aggression against US regional allies, major power war, and an increased risk of nuclear escalation.

Implications

Future scholarship should incorporate geopolitical conditions and the related foreign policy goals of the states in question when theorizing the effects of technology on international politics. Often scholars attempt to conceptualize the effects of weapons systems in isolation from the political context in which they are embedded.

Studies treat technology as disembodied from geopolitics and as exerting independent effects on the international system. But technology does not float freely. Technology is a tool different actors can use in different ways. Bakers and arsonists employ fire in their crafts to strikingly different ends. In the current international environment, Russia and China would tend to employ technology toward advancing revisionist aims. Technological advances in these countries are therefore much more likely to disrupt the prevailing international order and nuclear strategic stability.

This approach also suggests the potential threat new technology poses to nuclear strategic stability is more pervasive than previously understood. To undermine strategic stability, new technology need not directly impact strategic capabilities. Rather, any technology that promises to shift the local balance of power in Eastern Europe or the Indo-Pacific has the potential to threaten nuclear strategic stability. [end page 69]

This understanding of this issue leads to different policy prescriptions. If the technology itself is the problem, then it must be controlled and should not be allowed to spread to any states. In contrast, the framework outlined here suggests a different recommendation: preserve the prevailing balance of power in Europe and Asia. Technological change that, on balance, reinforces the prevailing international system should strengthen stability.

Leading democracies, therefore, should increase investments in emerging technology to maintain a technological edge over their adversaries. Export control and nonproliferation measures should be designed to deny emerging military technology to Russia and China. Arms control should be negotiated with the primary objective of sustaining the current international distribution of power. Making progress in these areas will be difficult. But the consequences of failure could be shifts in the international balance of power, conflict among great powers, and an increased risk of nuclear war.

#### NATO EDT superiority will cement effective deterrence — quickly getting innovative tech to the battlefield is key.

Hodges 21 — Ben Hodges, Pershing Chair in Strategic Studies at the Center for European Policy Analysis, Retired Lieutenant General in the U.S. Army where he served as Commanding General of the United States Army Europe, Senior Associate Fellow at the Royal United Services Institute for Defense and Security Studies (UK), 2021 (“Defense Technologies… for What? Speed, Speed, Speed!,” Center for European Policy Analysis, February 17th, Available Online at https://cepa.org/defense-technologies-for-what-speed-speed-speed/, Accessed 07-10-2022)

Giving our armed forces the proper technologies to perform their mission will ultimately ensure that deterrence never fails.

The key to effective deterrence for the transatlantic alliance is speed: speed of recognition of the Kremlin’s malign activities; speed of decision to start necessary deployments, movements and related activities; and speed of assembly to move faster than the Kremlin to pre-empt attacks and signal our preparedness to act. Fortunately, a wide range of new technologies are emerging and evolving that can improve speed, if they are properly integrated into our armed forces and into our plans.

New technologies that have the greatest potential to this end include artificial intelligence, machine learning, automated systems, hypersonics, and cyber technologies, among others. All these tools can enhance decision-making, improve interoperability of mission command systems and logistics, help counter adversaries’ unmanned air and maritime systems, and facilitate material changes to improve military mobility. Key to maximizing the impact of these new technologies, and to making the investment worthwhile, is coordination among political decision-makers and industry innovators to understand Allies’ needs and meet capability requirements.

Below are some examples of those needs and corresponding technological requirements. Though in need of refinement, these provide an azimuth for innovators, policymakers and industry leaders across the transatlantic community to improve our collective speed and enhance effective deterrence.

Need for Speed of Recognition: Recognizing threats, indicators, and warnings from our adversaries has become increasingly difficult within the context of hybrid warfare. Unlike in the Cold War, when the first indicator of an attack may have been T72 tanks coming over the horizon, today, the first indicator may be a cyber-attack that shuts down transportation or financial systems. It could be a dockworkers’ strike in a Baltic port, or even attacks on transportation infrastructure by hypersonic missiles. Being able to see these possibilities as they are taking shape, before they are effective, is necessary to prevent or respond to an emerging crisis.

Requirement: Technologies that can fuse the wide range and variety of intelligence and information as part of NATO’s indicators and warnings network are vital. A U.S. satellite will most likely not be the first system to detect a hybrid threat or activity. Instead, it could be a human source, perhaps a customs agent, border guard, or member of a territorial force. But how does information about a dockworkers’ strike in a Baltic port turn into analysis, for instance, that reveals this strike was created artificially by FSB operatives to create a pretext for the Kremlin to interfere abroad? The key lies in the ability to quickly and accurately parse through all available data and reports — across national and interagency boundaries, NATO and non-NATO nations, five-eye and non-five-eye nations — using artificial intelligence, machine learning, and other fusion capabilities. This also requires protecting information networks from hacks, malware, and other attacks, all the while facilitating the sharing of sensitive and classified information, using sophisticated cyber defenses.

Need for Speed of Decision: Authorizing movements and actions to prevent or respond to an emerging crisis, within a NATO context, requires the unanimous consent of all 30 member states. Decisions to start moving capabilities, pull ammunition such as Patriot “Interceptors” out of storage depots, and reprioritize military movements, demand high-level decision-makers to act quickly and decisively, despite the sensitive nature of these activities. The Kremlin is fully aware of NATO’s decision-making process, the requirement for unanimous consent, and the political reluctance to delegate such decisions about movement to operational commanders, and they aim to exploit that gap through their own centralized decision-making.

Requirement: This means Allied and partner political decision-makers need to have access to a variety of information, plans, options, and shared courses of action to create appropriate signals and communicate tasks to commanders in a timely manner. That’s why it’s critical to leverage technologies such as synthetic environments and human augmentation, which can enable Allied political leaders to simulate complex, multi-domain environments, test time-sensitive decision-making, and physiological responses, and course-correct in advance through sustained exercises and training.

Need for Speed of Assembly: NATO must demonstrate that allies are able to move as fast, or faster than, Russian Federation forces to prevent or react to an emerging crisis. The key is signaling to the Kremlin that any malign activities will either fail or be too costly to attempt. Still, NATO must do this in such a way that it does not unnecessarily provoke or escalate tensions with Russia. This requires assembling key forces and capabilities quickly and strategically in pre-crisis or peacetime conditions.

Requirement: In order to assemble fast enough, technologies are needed to protect against cyber-attacks against transportation and power-generation infrastructure and reduce the weight and size of modern armored vehicles which are difficult to move quickly across the continent to the frontline. Using technology to develop affordable bridging assets necessary for the many river crossings in Europe, as well as to protect against Russian unmanned systems and create a NATO anti-access aerial denial (A2AD) bubble, should be priorities. Automated systems — from robots and drones to active cyber defense as well as new missile technologies — can play crucial roles in protecting allied and partner deployments and critical infrastructure.

At the end of the day, deterrence depends on the women and men of our armed forces being trained and ready. Giving them the proper technologies to perform their mission will give them the advantages needed to improve awareness, preparedness, and speed and, ultimately, ensure that deterrence never fails.

#### NATO deterrence prevents global hotspot escalation and great power war.

Dowd 22 — Alan W. Dowd, Senior Fellow in the Center for America's Purpose at the Sagamore Institute—a think tank, Senior Fellow at the Fraser Institute and the American Security Council Foundation, Contributing Editor and Columnist at the American Legion Magazine, former Adjunct Professor of American Foreign Policy at Butler University and Anderson University, 2022 (“Putin’s war, NATO’s unity, Ukraine’s valor,” *American Legion Magazine*, March 15th, Available Online at https://www.legion.org/landingzone/255256/putin%E2%80%99s-war-nato%E2%80%99s-unity-ukraine%E2%80%99s-valor, Accessed 04-04-2022)

**[\*\*\* Note: 9/11 refers to the September 11, 2001 terrorist attacks against the United States; 11/9 refers to the November 9, 1989 fall of the Berlin Wall.]**

Vladimir Putin’s “unprovoked, unjustified, unconscionable war” has taken thousands of lives, destroyed much of Ukraine’s modern infrastructure and ancient landmarks, and created the largest tidal wave of refugees in Europe since World War II. Yet amidst all these horrors, there’s a flicker of hope: The NATO alliance is more united than at any time since 9/11 – and more important than at any time since 11/9. This is the very opposite of what Putin expected.

Common cause

Consider how the 30-member alliance swiftly rejected Putin’s December demands that NATO not expand to include Ukraine, cease its deterrence operations in Eastern Europe and grant him veto authority over the decisions of sovereign nations. Then, as Putin massed more than 180,000 troops, hundreds of tanks and dozens of warships on Ukraine’s borders and coasts, the alliance set about the task of bolstering its easternmost members.

The United States deployed B-52s to Britain; F-35s to Germany, Lithuania and Estonia; F-15s to Poland and Estonia; F-16s to Romania; dozens of AH-64 attack helicopters to the Baltics and Poland; Patriot air-defense batteries and thousands of combat troops to Poland; an armored brigade combat team of 7,000 soldiers to Germany; hundreds of troops to Hungary, Bulgaria and Romania; and 800 combat troops to the Baltics. There are now about 100,000 U.S. troops standing guard all across Europe.

In addition, Washington approved a long-delayed sale of 250 M1A2 tanks to Poland, and surged the aircraft carrier USS Harry S. Truman to join carrier strike groups from Italy and France in a show of force in the northern Mediterranean.

Britain has deployed hundreds of troops to Poland, sent warships to the Black Sea and eastern Mediterranean, dispatched Challenger tanks to the Baltics, doubled its troop commitment in Estonia, and based fighter-bombers in Romania and Poland. Canada has deployed hundreds of additional troops to augment its battlegroup in Latvia. Germany has sent troops to reinforce its contingent in Lithuania. France has deployed hundreds of troops to Romania. Germany and the Netherlands sent Patriot batteries to Slovakia. Denmark rushed F-16s to Lithuania and sent a frigate to the Baltic Sea. Dutch F-35s and Spanish Eurofighters deployed to Bulgaria. NATO now has 130 warplanes on “high alert” in Central and Eastern Europe, more than 200 ships forward-deployed in the waters of the Arctic, North Atlantic, Baltic, Aegean, Adriatic and Mediterranean, and tens of thousands of newly deployed or repositioned combat troops in the region, according to NATO Secretary General Jens Stoltenberg.

For the first time in history, NATO activated and deployed its rapid-response force. And for just the second time in history, Turkey – acting under international authorities it was granted by a 1936 treaty – closed the Black Sea to Russian warships.

NATO hasn’t limited its response within its footprint. In a ~~crippling~~ [crushing] blow to Russia’s economy, NATO members, the EU, Japan and other partners disconnected Russian banks from SWIFT, the global messaging system that enables financial transfers among 11,000 banks in 200 countries. Britain, Canada and the European Union joined the United States and other partners in imposing “unprecedented export control measures” to cut off Russia’s access to high-tech products. The allies closed their airspace to commercial and private Russian aircraft, seized Russian assets, and cut off Putin’s kleptocracy from the most of the world.

Specific to Ukraine, before the invasion, the United States flew reconnaissance flights over eastern and western Ukraine, shared intelligence with Kiev, and formed an airbridge linking NATO bases with Ukraine. This enabled delivery of defensive weapons from North America, Britain and Europe.

When Russia started to fill Ukraine’s skies with missiles and artillery, NATO began delivering weapons overland. In the first six days of the war, the alliance rushed 17,000 antitank weapons into Ukraine. The United States has shipped tons of small-arms ammunition, mortar and artillery shells, Javelin antitank systems, Stinger anti-aircraft systems, and grenade launchers. Britain has delivered 3,615 antitank systems, as well as Starstreak antiaircraft missiles. The Baltic nations have sent antiaircraft missiles and antitank systems. Poland sent antiaircraft weapons. Turkey has delivered ground-attack drones. In a stunning reversal, Germany rushed 2,000 antitank weapons and 500 surface-to-air missiles to Ukraine. Non-NATO member Sweden delivered 5,000 antitank systems to Ukraine’s gallant defenders.

Challenges

Even so, Putin’s war on Ukraine has exposed challenges within NATO. The most glaring of these revolve around Germany – namely, Berlin’s equivocation over the future of the Russia-to-Germany Nord Stream 2 gas pipeline and Berlin’s decision to block delivery of German-built weapons to Ukraine. These policies prompted some observers to ask those eternal questions: “Is NATO broken, and is it worth the trouble?”

The answer to that first question is found in the above paragraphs. It’s impossible to read Putin’s mind, but the rapidity and unity of NATO’s response surely came as a surprise to the Russian strongman. Indeed, NATO’s response the past 70 days represents the very opposite of what happened when Putin mounted his first invasion of Ukraine in 2014.

The fact that NATO didn’t prevent Putin from moving against Ukraine isn’t a NATO failure; it’s a function of the harsh geopolitical reality that Ukraine is not a member of the most important, most enduring security alliance in history. To be sure, Europe will be more stable – and NATO more secure – if Ukraine can somehow remain a sovereign, democratically oriented nation. That explains why the alliance worked so hard on the diplomatic and military front to make Putin think twice about this criminal invasion.

However, the central purpose of NATO is to deter an attack against its members and, if necessary, to defend its members from attack. Indeed, the fact that Putin has attacked Ukraine while keeping his hands off NATO members Estonia, Latvia, Lithuania and Poland underscores that he respects NATO’s all-for-one security guarantee – at least for now.

In these weeks of war, Ukraine has shown itself to be a nation of warriors and a worthy ally. Its Churchillian leader and courageous people have earned NATO’s respect – and if they survive the hell Putin has unleashed, a seat at NATO’s table. But Russia's sheer mass could be enough to overwhelm Ukraine, especially as Putin employs the beastly scorched-earth tactics he perfected in Chechnya and Syria.

Headaches

As to whether the alliance is worth the headaches and heartburn it causes – especially for the United States – the answer to that question is found in both the historical record and today’s headlines.

To be sure, Germany’s prewar resistance to sending defensive weapons to Ukraine frustrated its NATO allies, and Germany's dependence on Russia’s natural gas has proven to be shortsighted. But it pays to recall that NATO overcame far more worrisome internal challenges in the past. Consider the Anglo-French deceptions during the Suez crisis in 1956, France throwing out NATO’s headquarters and pulling out of NATO’s integrated military command in 1966-1967, open hostilities between Turkey and Greece in the 1970s and 1980s, and France and Germany waging a diplomatic war against the United States and Britain in 2002-2003 over Iraq’s repeated violations of U.N. Security Council resolutions.

In spite of all of that, NATO repeatedly proves its importance to America’s security. Too many Americans forget or simply don’t know that NATO is a force-multiplier for U.S. power, a bridge to global hotspots, a backstop against great-power war in Europe, and a ready-made structure where like-minded nations with shared values and high levels of military interoperability build coalitions to defend their freedom and interests. These alliances within the alliance helped the United States liberate Kuwait, defend Saudi Arabia, wage war and keep peace in the Balkans, avenge 9/11, topple Saddam’s regime and respond to COVID-19.

Moreover, Germany has now suspended Nord Stream 2. As noted, Germany has rushed thousands of weapons systems to Ukraine. And in a truly remarkable about-face, Germany is increasing its annual defense outlays to 2% of GDP (something Washington and NATO have been begging Berlin to do since 2006), creating a $112.7 billion modernization and rearmament fund, and building a strategic LNG reserve and new LNG terminals.

“The world,” German Chancellor Olaf Scholz concludes, “will no longer be the same as the world before.” Or perhaps more accurately, Europe and the world are returning to what they were before 11/9, when the Berlin Wall collapsed.

Insurance

Throughout the post-Cold War period, the alliance served as an insurance policy, just in case Moscow reverted to its old ways. And here we are.

Insurance is a good way to understand NATO. Insurance, after all, is about providing protection against worst-case scenarios. Prudent people hope they never have to use insurance, but they realize that paying a little each month or each year protects them against having to pay a lot – or losing everything – if disaster strikes. The same is true in the realm of international security.

The deterrent represented by Article V of the North Atlantic Treaty serves as insurance against worst-case scenarios. For America, NATO is a hedge against another European conflict triggering another continentwide or worldwide war. For NATO’s other members, NATO is a security guarantee backed by America. Without that guarantee, there’s no security, as history has a way of reminding those on the outside looking in, from Cold War Hungary to post-Cold War Ukraine.

Like all insurance policies, there are costs associated with NATO. A recent study revealed that U.S. defense expenditures earmarked for Europe amount to $36 billion per year. That’s not a trivial amount of American taxpayers’ money. But consider what America gets in exchange for that insurance premium: a hedge against another Argonne or Normandy, a Europe reinforced against invasion, and economic benefits that exponentially exceed those premium costs.

With Putin trying to reconstitute the Russian Empire and reverse the settled outcomes of Cold War I, NATO is proving its worth yet again. As Gen. James Mattis puts it, “If we did not have NATO today, we would need to create it.”

#### The NATO Innovation Fund (NIF) and defense innovation accelerator (DIANA) are good first steps, but additional U.S. support is key to actualize their benefits.

Nelson 21 — Nicholas Nelson, Non-Resident Senior Fellow for Emerging Tech and Policy with the Transatlantic Defense and Security Program at the Center for European Policy Analysis, Senior Technology Advisor at the Georgia Tech Research Institute, 2021 (“Getting NATO Innovation Right,” Center for European Policy Analysis, June 18th, Available Online at https://cepa.org/getting-nato-innovation-right/, Accessed 07-03-2022)

The Defense Innovation Accelerator and NATO Innovation Fund announced at the NATO Summit are welcome developments, but they require new authorities and differentiated talent.

Swift technological change has meant governments and the military created new organizations and approaches to innovation and rapid acquisition. Unfortunately, many do not have the necessary authority, budget, or workforce to succeed, meaning that meaningful change and impact have been sacrificed for theater. For the newly announced Defense Innovation Accelerator North Atlantic (DIANA) – with planned locations in Toronto and Cambridge, UK – and the NATO Innovation Fund (NIF) to succeed, they must address authority and budget concerns, and then bring in the right personnel to lead and staff them.

Authorities

There are three key authorities that NATO must get right for DIANA and NIF: reporting lines, patience (or willingness to accept failure), and decision making.

\* First, DIANA and NIF should operate independently with a direct line into the most senior decision-makers (the Secretary General, SACEUR, Supreme Allied Commander Transformation — SACT, etc).

\* Second, they need to be allowed to fail. The most impactful defense organizations (and indeed commercial organizations, particularly in the startup world) normalize taking big bets, with the knowledge that many will likely fail, and even the ones that succeed may take years to realize their full impact.

\* Third and finally, these new NATO bodies need to invest in or provide support to initiatives and startups without requiring external permission or consensus. At the same time, they also need a clear transition partner for promising capabilities to be handed off to (e.g. DARPA transitioning tech to the U.S. Department of Defense), which can move from development to deployment. This will enable the Alliance to more readily identify, develop, and deploy emerging and disruptive technologies.

Similar efforts including the U.S. Department of Defense’s DARPA and Defense Innovation Unit, CIA’s In-Q-Tel, and USAF’s Strategic Capabilities Office, are effective because they exist outside of traditional bureaucracies, leverage non-traditional talent strategies, and have consistent budgets.

Budget

Allocating funding seems obvious, but too often limited forethought is given to this issue. To ensure success, organizational funding must be significant, multi-year, and consistent or include inbuilt annual growth. A number of high-potential initiatives have either been announced with no dedicated funding or have had sizable funding gaps in subsequent years damaging their brand and relationships with defense companies and startups alike. The NIF in particular will likely rely on the willingness of Alliance members to make contributions beyond other NATO obligations. If so, multi-year commitments are crucial, as are success metrics, such as return on investment, which are rarely used within NATO or national government departments.

Talent

Finally, and most overlooked, is getting talent right. External talent is crucial. It is not enough to simply construct new organizations staffed in the traditional manner. To realize their full potential, NATO must attract talent with startup and/or venture capital (VC) experience, and pair them with top subject-matter experts from R&D communities, both government, and commercial. This cannot be done with NATO’s current Byzantine, long, drawn-out hiring process, which can last six months or even longer, and advantage insiders versus external candidates. As such the Alliance must engage and attract this talent. The good news is NATO has a number of potential examples to draw on for potential hiring pathways. In the U.S. the Defense Digital Service hires design and technical experts for one-to-two “tours of duty,” using their skillsets and operate outside the traditional civil service. In the UK, strategy and technology professionals are seconded into the Ministry of Defence, the Department of Trade, and intelligence organizations such as GCHQ, to provide experience or skills that may not exist within the current civil service workforce.

But providing pathways alone is not enough: attracting this talent to apply and convincing them to join is just as important. This requires identifying areas where they might work, including industry, academia, and startups, and VC. At the same time, other steps are needed. Upskilling existing NATO civilians – among the international and international military staff (IS and IMS) — and Alliance service members are needed to address this skill and understanding gap. To do so, it is helpful to expose them to startup and VC environments. Programs like Shift’s Defense Ventures Program in the U.S. have succeeded in building understanding between the Department of Defense’s civilian and military workforce and startups and VCs. They’ve done so by bringing in high-performing defense personnel for eight-week immersions with growing venture-backed startups or VC firms. This cultivates the necessary connective tissue between startups, VCs, and the military. NATO could readily follow a similar process by providing its highest performers the opportunity to temporarily work alongside leading North American and European startups and investors.

What’s Next?

Accelerating the development, deployment, and integration of emerging and disruptive technologies into the strategic and tactical environments is at the core of future NATO operations. The Alliance’s move to build DIANA and NIF, along with incorporating the right language into strategic documents are significant first steps. But building these initiatives from scratch will require significant planning to establish the right authorities, budget, and talent environment to enable these organizations to thrive. In order to do so, they need to build outside of traditional NATO structures and models while creating a differentiated talent and organizational culture.

#### Specifically, increased U.S. security cooperation with NATO is vital to NIF and DIANA effectiveness.

Long 22 — James E. Long, Colonel in the United States Air Force, National Security Fellow with the Defense Project at the Belfer Center for Science and International Affairs at Harvard University, holds an M.S. in Space Studies from the American Military University, 2022 (“How the US Can Assist NATO and its European Alliance Members in Addressing the China Security Challenge,” Harvard University Belfer Center Defense Project Paper, June, Available Online at https://www.belfercenter.org/sites/default/files/files/publication/DefenseProject\_National%20Security%20Fellowship\_v3\_220624.pdf, Accessed 06-25-2022, p. 24-25)

4. The US should help NATO create R&D centers and defense innovation hubs to harness emerging technologies being developed by allies.

As was noted in the NATO 2030 Reflection Group, China is making rapid advancements in telecommunications, space, cyberspace, and other new technologies with the intent to be the world leader in AI by 2030 and the world’s leading global technological superpower by 2049.96 In response, NATO issued its 2030 Agenda that seeks to increase NATO transatlantic innovation and technological edge while preventing innovation gaps among allies.97 Moreover, the NATO Advisory Group on Emerging and Disruptive Technologies (EDT) issued a 2020 report citing pathways for NATO to become an EDT-ready organization, recommending that NATO establish a network of innovation centers [or defense innovation hubs] throughout NATO with funding to match.98

As a result, during the 14 Jun 2021 Brussels summit, NATO issued a communique announcing the establishment of a NATO Innovation Fund to promote transatlantic startups and a Defense Innovation Accelerator for the North Atlantic (DIANA). Since DIANA is intended to be NATO’s version of the US Defense Advanced Research Projects Agency (DARPA), the US is in a very good position to promote transatlantic coordination on AI, big-data processing, quantum-enabled technologies, autonomy, biotechnology, hypersonic weapons, and space.99 In addition, the US could support the Innovation Hub by helping pre-vet investors to ensure allied technology would be protected from illicit transfers.”100

Accordingly, the US should support NATO by helping create R&D centers and defense innovation hubs that could better harness emerging technologies to support NATO allies. These centers and hubs would help accelerate technology and improve cooperation among NATO allies and partners and would heavily rely on partnerships with academia, researchers, industry, and start-ups.101 Linked to these NATO centers and hubs would be universities, commercial [end page 24] sector, and allied countries’ organizations that accelerate technology into the hands of the warfighter. For example, the US has several organizations, such as DARPA, Defense Innovation Unit, AFWERX, SPACEWERX, Army Futures Command and NavalX, that could coordinate closely with NATO centers and hubs to collaborate on similar problem sets and solutions.

Another important facet of these NATO centers and hubs is assessing how the technology will impact NATO’s ability to jointly fight in the future. The NATO R&D Center would need to be linked to NATO’s Allied Command Transformation in Norfolk, Virginia, to identify potential impacts of the technology on NATO’s war-fighting capabilities. Accordingly, the US should work closely with NATO allies to ensure integration and interoperability with these new technologies.102

#### U.S. expertise and capabilities are key to quickly get required tech to the battlefield — U.S. cooperation will streamline NATO’s innovation pipeline.

Cook and Dowd 22 — Cynthia R. Cook, Senior Fellow and Director of the Defense-Industrial Initiatives Group at the Center for Strategic and International Studies, former Senior Management Scientist and Director of the Acquisition and Technology Policy Center at the RAND Corporation, holds a Ph.D. in Sociology from Harvard University, and Anna M. Dowd, Co-Founder of Digital Innovation Engine—an organization working on technology innovation, Adjunct Scholar at the RAND Corporation, former Principal Officer for Strategic Partnerships and Head of Industry Relations at the NATO Communications and Information Agency, former Fellow at the European Union Institute for Security Studies (France), holds an M.A. in International Relations from the Warsaw School of Economics (Poland) and a joint M.A. in European Studies from the Warsaw School of Economics (Poland) and Sciences Po (France), 2022 (“How to Get NATO Forces the Technology They Need,” *War on the Rocks*, May 13th, Available Online at https://warontherocks.com/2022/05/how-to-get-nato-forces-the-technology-they-need/, Accessed 07-12-2022)

In a Feb. 26 Twitter post, Mykhailo Fedorov, Ukraine’s vice prime minister and minister for digital transformation, asked the SpaceX chief executive, Elon Musk, to provide Ukraine with Starlink terminals to enable satellite-based communications. In less than 48 hours, Starlink user kits arrived in Ukraine, immediately improving the command-and-control ability of Ukraine’s military.

For those of us who study the NATO acquisition process, it is almost impossible to imagine the alliance identifying a requirement and adopting a solution so quickly, no matter how urgent the circumstances. Among the many challenges would be the alliance’s elaborate, consensus-based governing structure, as well as the divergent interests and funding mechanisms among the 30 member states. This is why, in 2016, the International Board of Auditors concluded that NATO struggles to provide commanders with required capabilities on time and estimated that common-funded capabilities required an average of 16 years from development to delivery.

The complexity of modern weapons systems and the challenges of interoperability mean that any active engagement will lead to the identification of new technical requirements for NATO. The alliance needs the processes and structures in place to rapidly identify these requirements and procure solutions. This includes giving commanders the authority to make decisions without the lengthy consensus-building approach that may be reasonable, if slow, in peacetime but is not effective during war.

First Steps

NATO has previously sought to improve the governance, speed, and efficiency of its capability-delivery process. For example, in 2018 NATO adopted a new governance model for common-funded capabilities. It has undertaken efforts to enhance collaboration between strategic commands (Allied Command Operations in Mons, Belgium and Allied Command Transformation in Norfolk, VA), called for the exploration of alternative acquisition strategies to support technology development, and created the Office of the Chief Information Officer to accelerate the delivery of computer and information systems. Furthermore, in October 2021 NATO launched the first $1.1 billion Innovation Fund, and last month announced the creation of the first ever Defense Innovation Accelerator for the North Atlantic to harness cutting-edge technologies as part of the NATO 2030 agenda.

These are valuable steps, but they do not address the fundamental challenge of rapidly acquiring common capabilities. There are still many residual processes where consensus-based control is inherently prioritized over speed, flexibility, innovation, and the deployment of prototypes at the end of their development phases.

NATO leaders recognize the ongoing challenge. In a recent speech to the North Atlantic Council, the supreme allied commander transformation, Gen. Philippe Lavigne, stressed that one of his key priorities is to ensure the timely delivery of new and critical capabilities, adding that “we need to change the rules and make them work for us, not against us.” But NATO leaders cannot fix this alone — the alliance’s 30 member nations are the ones that will have to agree on the solution. Exploring alternatives and getting the allies to agree on a solution will be difficult. It can happen on a NATO-wide basis, or some subset of member nations can take on the challenge and lead the effort, which may then be adopted by others.

What Works

Access to adequate funding is a necessary starting point, and NATO has a track record of funding common capabilities. In 2021, NATO was implementing over 3,000 common-funded projects, worth approximately $17 billion (of which the United States funds about 22 percent). These include providing critical technology that supports the planning and execution of all NATO air operations, and the Air Situation Data Exchange that enhances situational awareness at NATO’s borders with partner nations, including Ukraine.

But the capability-fielding process is still subject to delays, which would be dangerous when addressing needs identified during combat operations. To avoid this, alliance members should commit to providing funds for a rapid-acquisition organization on a preauthorized and discretionary basis, in essence creating a bank account that can be drawn upon when needed. Even if this were a credit line that members committed to, rather than a standing pot of funds, it would limit setbacks caused by the slow and political processes of identifying and appropriating funding.

Ensuring adequate funding is not the only answer. Commanders also need the authority to streamline the identification of urgent needs and a standing mechanism, not an ad hoc approach, that can provide the flexibility and authority to address them. This exists for some alliance members on a national basis. The commander of the Dutch Defense Materiel Organization’s Computer Emergency Response Team, for example, has a pre-authorized budget and the power to expedite acquisitions of up to 500,000 euros for urgent cyber capabilities within 14 days. However, there is no NATO-wide approach.

The U.S. Department of Defense offers a variety of acquisition approaches that NATO could draw from. The United States has a model where the military services are largely responsible for acquiring weapon systems and providing them to the joint force commanders. There are also several Department of Defense organizations that have been stood up to address cross-service challenges. This means that there are both joint department-wide and service-level acquisition organizations procuring materiel to serve as examples.

Over time, the Department of Defense has developed processes to allow requirements identified on the battlefield to be quickly addressed. Different parts of the department have also embarked on different forms of organizational innovation.

One example is the Air Force’s Rapid Capabilities Office, which was formed in 2003 to “expedite important, often classified programs while keeping them on budget.” The office has a unique management structure — it reports to a board of directors that is chaired by the undersecretary of defense for acquisition and sustainment and includes the most senior leaders of the Air Force and the under secretary of defense for research and engineering. These senior leaders can both set priorities for spending and work to find the necessary funding. Furthermore, acquisition experts at the Rapid Capabilities Office are carefully selected to maintain a culture where “lean, agile, and forward-looking technology development” is possible. Along with the Air Force’s new stealth bomber, the B-21 Raider, the office oversees the X-37B Orbital Test Vehicle, “an experimental test program to demonstrate technologies for a reliable, reusable, unmanned space test platform.” The effectiveness of the Rapid Capabilities Office is affirmed by the decision to put these two extremely important programs there rather than within more traditional Air Force acquisition organizations.

Another concept comes from the Defense Innovation Unit, which was designed to work across the Department of Defense to identify and understand critical national security challenges that can be solved with leading-edge commercial technology within 12 to 24 months. The Defense Innovation Unit connects with non-traditional suppliers in innovation hubs, including Silicon Valley, and uses flexible acquisition models to issue contracts in as little as 2 to 3 months. It then publishes a catalog of commercial “solutions” ready for purchase from a range of companies, many of whom are not traditional defense suppliers. These include the Next Gen Explosive Ordnance Disposal Underwater Response Vehicle, a remotely operated underwater vehicle that searches for mines, and Hunt Forward, a set of tools for forward-deployed cyber operations. Although implementation has not always been smooth, the Defense Innovation Unit has nonetheless provided battlefield commanders with a range of innovative solutions that they can turn to.

The Rapid Capabilities Office empowers its leadership to finalize requirements and rapidly commit funding, a crucial component of its success. The Defense Innovation Unit focuses on creating a pipeline of new technologies. And these organizations are not unique. There are others across the services, such as NAVALX, the Army Applications Lab, and AFWERX, that are aimed at adapting innovations from both traditional and non-traditional suppliers. The United Kingdom’s Royal Air Force has its own Rapid Capabilities Office, which has also shown promise.

These U.S. models prove that a bureaucracy as resistant to change as the Department of Defense can still develop new organizational structures and processes. The Dutch and British models show that attempts at organizational innovation are not limited to the Pentagon. NATO may choose to adapt one of these or to develop its own unique approaches. The goal should be to provide its commanders with the flexibility and the authority to “validate requirements” — that is, to formally approve what the warfighter needs to execute the fight — and to make resources available. The decision structure could be a small rotating board of senior leaders, perhaps with time limits for approving or rejecting requirements to force rapid decisions.

NATO also needs a way to connect with industry partners across the alliance, capitalizing on innovations from small businesses and startups using new and flexible contracting mechanisms. The alliance currently lacks the tools to rapidly adopt commercial technologies. Two related policies would help to enhance the ability of new technologies to connect with existing systems. To increase operational effectiveness, NATO should leverage interoperability standards that allow different systems to operate seamlessly in a multi-domain environment. A related approach would be to adopt open systems architecture approaches for NATO weapons. This would provide design information to companies for developing components that could work with existing systems using a “plug and play” approach. Both of these policies would build upon the traditional NATO strength of developing standards while making these standards relevant to innovative companies.

All these process changes and organizational innovations will take effort — and the journey may be slowed by NATO’s consensus-building culture. Transformation takes time, but it only begins when there is a clear case for change. The scale and scope of Russia’s attack on Ukraine provides that case, and the delivery of Starlink provides an example of what could be possible if NATO had a more flexible approach to acquisitions.

#### Integrating the U.S. and NATO’s EDT innovation networks is key to burden-sharing and interoperability — allies “say yes.”

Kliman and Thomas-Noone 18 — Daniel Kliman, Senior Fellow in the Asia-Pacific Security Program at the Center for a New American Security, former Senior Adviser for Asia Integration at the U.S. Department of Defense, former Senior Advisor at the German Marshall Fund of the United States, holds a Ph.D. in Politics from Princeton University, and Brendan Thomas-Noone, Research Fellow at the United States Studies Centre at the University of Sydney (Australia), former Research Associate in the International Security Program at the Lowy Institute (Australia), holds an M.A. in International Relations from the University of Melbourne (Australia) and an M.Sc. in Global Politics from the London School of Economics and Political Science (UK), 2018 (“Now is the time to take DIUx global,” *Defense News*, May 24th, Available Online at https://www.defensenews.com/opinion/commentary/2018/05/23/now-is-the-time-to-take-diux-global/, Accessed 07-11-2022)

The Defense Innovation Unit Experimental — the Pentagon’s signature effort to engage commercial technology startups ― is primed to go global. In fact, DIUx could become a key platform by which the United States and its allies and partners come together to address shared military challenges ― if its next managing director and supporters in the Pentagon and Congress are prepared to seize the moment.

Launched in 2015, DIUx reflected a growing realization that the U.S. military needs to more effectively leverage innovations developed in the commercial technology sector. Intended as a workaround to a sclerotic defense acquisitions process, DIUx came to rely on an obscure contracting authority to rapidly award prototype projects to innovative companies ― a welcome change to the Pentagon business models that never managed to align with the technology industry’s far faster pace.

By the end of the Obama administration, DIUx had expanded beyond Silicon Valley to two other U.S. innovation hubs — Boston and Austin.

Growth gave way to uncertainty following the 2016 presidential election, with observers questioning whether the new team would support DIUx, and Congress moving to restrict its access to funding. Since then, however, DIUx has won the support of key stakeholders. Secretary of Defense Jim Mattis visited DIUx in mid-2017 and offered an unequivocal endorsement of its mission to “accelerate commercial innovation to the war fighter.” Michael Griffin, the new undersecretary of defense for research and engineering, has also expressed backing for DIUx, which falls within his portfolio.

Congress has warmed somewhat to DIUx, though whether it will fund the White House’s requested plus-up remains uncertain. And DIUx has demonstrated its ability to do more than fund prototypes ― transitioning two projects into production contracts by the end of 2017.

Engaging commercial technology companies in the United States will ― and should ― remain the primary focus of the next DIUx managing director. However, with DIUx now on more solid political and bureaucratic footing, there is a unique opportunity to broaden its horizons.

Taking DIUx global could deliver multiple advantages. U.S. commercial technology companies do not hold a monopoly on innovations relevant to solving vexing military challenges. For example, Israel is a leading global provider of counter-drone solutions. A more internationally oriented DIUx could improve the U.S. military’s access to technologies generated by companies located on the soil of its allies and partners, and simultaneously enable their governments to more effectively harvest U.S. commercial technologies for national defense needs.

Many U.S. allies and partners would welcome the opportunity to plug into DIUx, given the diverse threats they confront ― from rising regional powers to terrorist networks ― and constraints on the resources they can dedicate to defense. At the political level, cooperation around DIUx could help strengthen America’s alliances and partnerships at a time of uncertainty, while also bolstering future military interoperability.

Looking ahead, the United States will need to identify new and innovative ways to share the burden with its allies and partners to maintain its technological advantage. Although the Pentagon will see a budget increase over the next two years, without legislative action, mandated budget cuts will return in 2020. A more internationally oriented DIUx could help to spread the costs of research and development. Over the long term, it could even evolve into the cornerstone of a commercial innovation-oriented defense technology network spanning the United States and its allies and partners.

With traditional forms of security cooperation like large-scale research and development projects and foreign military sales failing to keep pace with a rapidly evolving threat environment, such a network could enable the United States and its allies and partners to more effectively address shared national security challenges.

DIUx has taken limited steps to engage U.S. allies and partners. On the government side, these include welcoming a United Kingdom liaison officer and, reportedly, plans to host an Indian military representative. DIUx has also worked with a handful of foreign commercial technology firms.

Yet, beyond these initial steps, significant opportunity exists. To take DIUx global, the next managing director could pursue multiple, mutually reinforcing options.

The easiest would be for personnel from DIUx and the military services to conduct a series of roadshows to U.S. allies and partners. These roadshows would serve a dual purpose: to showcase the portfolio of U.S. firms that work with DIUx and to raise the awareness of DIUx among overseas companies that typically do not consider the Pentagon as a potential customer.

A second option would be to establish offices overseas in order to embed DIUx in key ally and partner innovation hubs. These offices could take various forms ― from a handful of DIUx personnel based in a U.S. embassy to a bilaterally staffed organization funded in part by the host nation.

DIUx offices overseas could function as points of coordination across U.S. alliances and partnerships, supporting efforts like the “Five Eyes” Technical Cooperation Program, but focus on technologies emerging out of the commercial sector in addition to national laboratories. Some key considerations for selecting a location would include a high density of companies working on cutting-edge technologies with national security relevance; commitment by ally and partner militaries to leverage technology developed in the commercial sector; and willingness of ally and partner governments to put up resources.

A third option would be to launch dedicated funds under DIUx with financing contributed from both the United States and its allies and partners to solve joint challenges. Each fund would focus on awarding prototype projects to companies with potential solutions to the challenge identified. This option would allow the United States and its allies and partners to share defense resources; provide more revenue to national security-relevant startups than the Pentagon could on its own; and build interoperability up front. A clear area for such a fund would be low-cost intelligence, surveillance and reconnaissance coverage over a vast maritime area ― a challenge that has long bedeviled the United States and Australia in the Indo-Pacific region.

The next managing director of DIUx will have an unparalleled opportunity to take it global. But she or he will need a mandate to do so ― ideally from the secretary of defense. With that mandate, the next managing director should quickly move to advance an ambitious agenda for involving allies and partners more closely in the work of DIUx. Announcing that DIUx will open an office overseas within a year would, in particular, galvanize ally and partner interest.

### 1AC — Plan

#### The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization to strengthen defense innovation hubs and research and development in artificial intelligence, biotechnology, and cybersecurity, including by substantially increasing its support for and participation in the NATO Innovation Fund and Defense Innovation Accelerator for the North Atlantic.

### 1AC — Alliance Fragmentation Advantage

#### Contention Two: Alliance Fragmentation

#### Current transatlantic EDT policy is fragmented — bridging the gap between the U.S., NATO, and the EU is key to effective innovation and interoperability.

Speranza and Jans 21 — Lauren Speranza, Director of the Transatlantic Defense and Security Program at the Center for European Policy Analysis, former Deputy Director of the Transatlantic Security Initiative at the Atlantic Council, holds an M.A. in International Security from the Brussels School of International Studies (Belgium), and Karlijn Jans, Defence Policy Advisor at the British Embassy in The Hague (Netherlands), former Strategic Analyst at the The Hague Centre for Strategic Studies (Netherlands), holds an M.A. in European Studies from King's College London (UK) and an M.A. in European Studies from the Humboldt Institute of Berlin (Germany), 2021 (“Bridging the Gap: Time for an EU-NATO Strategic Dialogue on Defense Tech,” Center for European Policy Analysis, February 17th, Available Online at https://cepa.org/bridging-the-gap-time-for-an-eu-nato-strategic-dialogue-on-defense-tech/, Accessed 07-10-2022)

To stay secure, the transatlantic community must take on emerging and disruptive technologies together.

Today’s transatlantic security hinges on technology. On both sides of the Atlantic, our militaries, societies, economies, and information systems require increasingly advanced technologies to stay better, faster, and stronger than our adversaries and competitors. To retain their advantage and address vulnerabilities, the United States and Europe must work in lockstep to harness emerging and disruptive technologies for their collective defense. The key is to employ NATO and the European Union (EU) in unison for strategic effect.

NATO, the EU, and their member states have recognized the urgent need to combine their complementary capabilities to contest Russia and China, especially in the technological domain. Just yesterday, NATO Secretary General Stoltenberg announced a new a Defense Innovation Initiative “to promote interoperability and boost transatlantic cooperation on defense innovation” among allies – 21 of which are members of both NATO and the EU. NATO and the EU also share an overlapping set of forces, capabilities, talent, intellectual property, and budgets for defense investment and research and development (R&D). Under the 2016 Joint Declaration, practical NATO-EU cooperation has been humming along, despite lingering political obstacles. Applying emerging and disruptive technologies (EDT), such as artificial intelligence (AI), autonomous systems, space capabilities, hypersonics, quantum tech, and human augmentation, for defense has been a key focus area. This has been underscored by, for example, jointly supported workshops at the European Center of Excellence for Countering Hybrid Threats (Hybrid COE) and NATO-EU senior military staff talks. As each organization has made EDT advances, staff-level coordination and broad information sharing have helped to better align their efforts. For instance, NATO’s EDT roadmap team, Innovation Hub, and Science and Technology Organization have engaged with the European Defense Agency (EDA)’s tech work.

But staff-level coordination can only bear so much fruit in the absence of a more robust political effort. As strategic and technological competition with Russia and China has intensified, the stakes have risen too high to settle for incremental activities. Avoiding the political battles required to forge a more meaningful joint NATO-EU approach, nations have begun exploring other transatlantic forums to address EDT issues. The Canadian and French-led Global Partnership on AI, the U.S.-led AI Partnership for Defense, and the European Commission’s proposed Transatlantic Tech and Trade Council are a few examples. Each of these platforms is useful in its own right, specifically for AI issues, and could benefit from NATO and the EU joining to add their institutional weight. The risk with this approach, however, is the rapid fragmentation of transatlantic efforts on EDT. If this trend continues, the result could be a diffused smattering of multilateral frameworks, each focused on a particular tech issue with a different small group of countries.

By opting for outside platforms, the transatlantic community misses the point. The added value of NATO and the EU is their ability to coordinate efforts among large groups of like-minded nations. Both institutions have a great deal of experience and infrastructure for doing so. On a transformative set of issues that requires a comprehensive approach, such as the defense application of EDT, NATO, and the EU have the capacity to make an enormous collective impact. Instead of scattering across alternative forums, interested member nations must find ways to drive their EDT work through a new NATO-EU mechanism.

Launching an EU-NATO Strategic Dialogue on EDT could be an important option to explore. Routine, higher-level meetings in this format would draw together senior representatives from each institution, as well as member states and the private sector — each of which plays vital roles in assessing vulnerabilities and shaping requirements for EDT. The scope should expand beyond AI alone to encompass consultations on the wider security implications of EDT. Tentative agenda items could include forging key principles for tech governance around the military applications of EDT; addressing data-sharing issues; coordinating defense R&D and investment incentives; and establishing more robust standards and technical requirements for EDT-enabled systems to enhance interoperability. This could potentially have positive spillover in better aligning EDT aspects of the EU Capability Development Plan (CDP), the Coordinated Annual Review on Defense (CARD), and the respective NATO Defense Planning Process (NDPP). It would also create synergies for the EU to leverage its budgetary and legislative tools, which NATO lacks, to more effectively reinforce the Alliance. Lastly, it could strengthen the collective “annual review of vulnerabilities in alliance critical infrastructure and technologies, including those stemming from foreign ownership and influence”, as the NATO Secretary General has proposed.

The plethora of applications of emerging and disruptive technologies in the defense realm is something that both militaries and policymakers are dealing with on a daily basis. Developments are rapid but, at the same time, require long-term engagement and vision from senior leaders. In the end, EDT not only has implications for soldiers on the battlefield, but also for political decision-makers. In the near term, the COVID crisis is occupying much of the bandwidth and institutional capacity across NATO and the EU, at the expense of accelerating the dialogue in support of defense innovation. But urgent action is needed to grow the transatlantic community’s fast-shrinking technological advantage in defense. It is paramount for leaders to diligently and intensively focus on this topic, as opposed to simply including it on the long list of issues for NATO or European Council meetings. Through a structured EU-NATO Strategic Dialogue on EDT, it could rightly become an integral part of the transatlantic meeting cycle, not least to create a common understanding around future defense implications. To this end, the NATO 2030 Reflection Group’s proposed NATO digital summit for governments and the private sector should be extended to EU stakeholders and ultimately feed into this strategic dialogue.

To stay secure, the transatlantic community must take on emerging and disruptive technologies together. It should be at the forefront of the joint action by the EU and NATO, reflecting the pressing need to act. This is of foundational importance for maintaining the Alliance’s strategic edge, addressing vulnerabilities of tech, and defending the norms and values it was built to protect. As the United States and Europe renew their collective agenda at the dawn of the new Biden administration, an EU-NATO Strategic Dialogue on Defense Tech should be at the top of their list.

#### Insufficient U.S. support for NIF and DIANA is driving this fragmentation — the plan is key to supercharge NATO-EU cooperation on EDT.

Besch 21 — Sophia Besch, DAAD/AICGS Research Fellow at the American Institute for Contemporary German Studies at Johns Hopkins University, Senior Research Fellow at the Centre for European Reform (Germany), Non-Resident Senior Fellow at the Atlantic Council Europe Center, Ph.D. Candidate in European Studies and Defence Studies at King's College London (UK), holds an M.Sc. in International Relations from The London School of Economics and Political Science (UK) and an M.A. in International Security from Sciences Po (France), 2021 (“Rebooting the U.S.-EU Defense Relationship,” American Institute for Contemporary German Studies, December 22nd, Available Online at https://www.aicgs.org/publication/rebooting-the-u-s-eu-defense-relationship/, Accessed 07-10-2022)

2. Align EU-NATO work on defense innovation and find new formats of engagement

Both the United States and the EU have an interest in investing in new and emerging defense technologies and to maintain interoperability, particularly in the context of the U.S. technology race with China. The United States, through AUKUS, has established an innovation partnership with just one European ally, the UK (for now). Meanwhile, NATO has launched a new defense innovation fund and a defense innovation accelerator (DIANA). The UK, which post-Brexit has given itself the guidance to ‘Think NATO,’[7] was a supporter of the Fund, but the United States and France are not members. At the same time, France often argues that the EU should be in the lead on emerging technologies and is pushing for the creation of an Innovation Defense Hub within the European Defense Agency. These defense innovation efforts pursued in parallel by both organizations are already leading officials to complain about NATO duplicating the EU and vice versa. Both Americans and Europeans should try to prevent a rehashing of this unproductive talking point.

Parallel to the EU branching out into ‘traditional’ security, NATO has been broadening its own understanding of security to include newer domains such as economic security, disruptive technologies, and disinformation.[8] This development provides clear opportunities for cooperation between the two organizations, but also presents risks of conflict and tension. NATO-EU cooperation today remains largely process-driven. Inter-institutional exchanges are often focused on ‘deconflicting’ rather than building genuine synergies,[9] and the relationship suffers from long-standing political conflict between Turkey and Cyprus and from newer tensions between the UK and France. The concurrent NATO Strategic Concept and EU Strategic Compass processes are an opportunity for the United States and the EU to work together to improve NATO-EU cooperation on innovation. The next NATO-EU joint declaration, which is scheduled to be published soon, could help by acknowledging a new division of labor between the two institutions.

For instance, it would make sense for the two organizations to cooperate on investment screening, research protection, and initiatives to facilitate information-sharing on dual-use export and import controls of critical technology.[10] These joint NATO-EU initiatives could usefully build on the work done by the United States and the EU at the Trade and Technology Council. On defense technology development, the Americans and Europeans could explore different new formats of engagement. For instance, the United States could expand AUKUS to include more European countries with relevant defense innovation profiles, such as France or Estonia. Or, if AUKUS remains too politically sensitive for Paris, the transatlantic allies could explore the possibility of the United States joining selected PESCO projects geared towards defense innovation. The United States may also want to reconsider its decision not to join DIANA.

#### U.S. support and participation is key to overall alliance coordination on EDT.

Mundell 22 — Ian Mundell, Innovation Reporter at *Science|Business*—a network of universities, companies, and research and policy organisations promoting innovation, 2022 (“The Ecosystem: in Europe, defence innovation is the new black,” *Science|Business*, June 7th, Available Online at https://sciencebusiness.net/news/ecosystem-europe-defence-innovation-new-black, Accessed 07-03-2022)

Suddenly, it seems, everyone cares about Europe’s defence innovation ecosystem. NATO is setting up the Defence Innovation Accelerator for the North Atlantic, or DIANA, with a significant presence in Europe. The European Commission is working on the EU Defence Innovation Scheme, EUDIS. And last month, Amazon Web Services announced it is setting up a private defence accelerator in the UK.

But details of the DIANA and EUDIS initiatives have been slow to emerge, leading to concerns that gaps and barriers to innovation remain to be addressed. EUDIS in particular leaves a lot of questions unanswered.

“It’s a step in the right direction, but whether it is enough is deeply debatable,” said Nicholas Nelson, senior fellow with the Transatlantic Defense and Security Program at the Center for European Policy Analysis in Washington DC. “And this will not be figured out in the next year or two. It will take five or ten years to see what the impact is.”

This sentiment is echoed by Alain De Neve, a specialist in defence innovation at Belgium’s Royal Higher Institute for Defence. “EUDIS is a timely initiative for the EU member states, although from a macro-strategic point of view there is still a long way to go for Europeans if they want to build a competitive research ecosystem on a more global scale,” he said.

Detecting hidden threats

EUDIS is intended to bring together all relevant EU initiatives that support defence innovation and entrepreneurship. This includes innovation-focused calls for proposals issued through the European Defence Fund (EDF), such as a planned technological challenge to test and mature technologies for hidden-threats detection, and a four-year partnership for the development of defence medical counter measures against chemical, biological, radiological and nuclear threats.

The Commission also plans a number of initiatives intended to structure the European defence ecosystem. Some of these are still frustratingly vague. There is to be a dual-use incubator to allow better spin-in and spin-out between the civil and defence sectors, and to spur technological maturation and adaptation. This project was first floated in the EU’s 2021 Action plan on synergies between civil, defence and space industries, which suggested it might be a virtual network based on close collaboration between the Commission, the European Innovation Council and the European Defence Agency.

At that stage, the incubator’s potential activities included screening EU-funded research for results relevant to defence and proposing them for follow-up funding or user uptake. It was also to support new technologies with dual-use potential coming from start-ups, SMEs, and research and technology organisations. But these details and partners have vanished from the latest description of the incubator, and the Commission says it has nothing more to add while preparations are on-going.

Detail is also still lacking on the cross-border innovation networks listed as part of the EUDIS toolbox. These are intended to test the relevance of technologies from the civil sector in defence-specific environments. Then there will be other supporting measures for innovative companies, such as matchmaking with primes, investors and end users; business coaching; and the organisation of hackathons.

Defence Equity Facility

The most concrete EUDIS initiative unveiled so far is the Defence Equity Facility, which is intended to address the lack of risk capital in the EU for start-ups and small and mid-size companies developing innovative defence technologies. The Commission will put €100 million into the facility over the next five years, which is expected to be augmented by the European Investment Fund and private investors to reach a total of €500 million.

“Enabling a better access to equity funding for innovative defence SMEs and mid-caps would support their growth and finally benefit to the innovativeness of the European defence technological and industrial base,” the Commission says in the latest EDF work programme, released on 25 May. “It will also reduce their exposure to non-EU investors and benefit to the EU’s strategic autonomy.” The creation of the facility is also intended to send a positive message to private investors that the EU’s defence sector is an attractive proposition.

Nelson thinks the Defence Equity Facility is a good start, but again a lot of important detail is still missing, such as how and on what terms the equity will be awarded. An enlightened choice would be to make non-dilutive investments, the approach used by Air Force Ventures in the US. “It is not taking equity, it is investing alongside private capital investors, because it views this as good for the ecosystem,” Nelson said.

But Nelson is also concerned that the facility potentially appears open to all-comers, rather than targeting start-ups and companies with a civilian background moving into defence. If confirmed, this will limit its impact.

For example, a seed round for a defence start-up might typically be around €2 million, with €500,000 from the Commission contribution required to lead the round. So, if the facility is focused exclusively on this early stage investment it might support 40 companies a year, which is modest enough. But if the facility gets involved in series A and B rounds, which might run to €5-7 million per round, its reach will be severely constrained. “To be honest, it needs to have another zero on the end per annum to have a catalysing effect,” said Nelson.

Gundbert Scherf, co-founder and managing director of Helsing, a German start-up active in artificial intelligence and software-defined defence, thinks this lack of focus is already holding back EDF. “Only 8% of EDF funds to date have been allocated to disruptive technologies. Consortiums primarily feature traditional primes instead of deep tech disruptors, who actually invest their own money into de-risking tech and hiring the right talent,” he said. “In reality we need to spend the majority of funds on disruptive technologies and empower new defence companies that are developing them. Only this will deliver the innovation, disruption, speed, and quality we need.”

Dual-use technologies

Another aspect of EUDIS that is unclear is how it will line up with NATO’s DIANA initiative. This was launched in April, with a mission to bring industry, start-ups and academia together to research new dual-use technologies. Initially it will run a network of more than 10 accelerator sites and over 50 test centres in innovation hubs across NATO alliance countries. The UK and Estonia will host DIANA’s European accelerators. Meanwhile, a complementary NATO Innovation Fund will invest €1 billion in early stage start-ups and other deep tech funds, over an unspecified period of time.

The Commission says that it will work with NATO “to ensure that we can develop synergies when and where possible”. De Neve thinks this may not be so straightforward. “It would be difficult to imagine that these two cooperation frameworks could operate without any exchange between them,” he said. “However, and to the extent that DIANA assumes the contribution of the US, it seems difficult to imagine interactions between these two institutions that do not clash with the restrictive measures put in place by the US in terms of transfer of sensitive technologies.”

#### U.S. security cooperation *with NATO* on EDT is vital to cement an alliance-centric framework that links transatlantic *and* Indo-Pacific allies.

Ford and Goldgeier 21 — Lindsey W. Ford, David M. Rubenstein Fellow in Foreign Policy at the Brookings Institution, Adjunct Lecturer in the Elliott School of International Affairs at George Washington University, former Richard Holbrooke Fellow and Director for Political-Security Affairs at the Asia Society Policy Institute, former Special Assistant for the US-ASEAN Defense Forum in the U.S. Office of the Secretary of Defense, holds an M.A. in Public Affairs and Asian Studies from the University of Texas-Austin, and James Goldgeier, Visiting Fellow in the Center on the United States and Europe at the Brookings Institution, Professor of International Relations at American University, former Professor and Director of the Institute for European, Russian, and Eurasian Studies at George Washington University, former Director for Russian, Ukrainian, and Eurasian Affairs at the U.S. National Security Council, holds a Ph.D. in Political Science from the University of California-Berkeley, 2021 (“Retooling America’s alliances to manage the China challenge,” The Brookings Institution, January 25th, Available Online at https://www.brookings.edu/research/retooling-americas-alliances-to-manage-the-china-challenge/, Accessed 07-10-2022)

Beyond building collective capacity to operate more seamlessly in response to today’s crises, the U.S. must also think more closely about building alliance innovation ecosystems for the future. With China set to overtake the U.S. in research and development spending — it already spends more on R&D than Japan, Germany, and South Korea combined — the U.S. and its allies will need to treat defense innovation as a combined task. Rising techno-nationalism and the lack of allied innovation networks will make this difficult absent intentional policy leadership. Looking forward, Washington should further expand new bureaucratic mechanisms such as allied R&D pools or defense innovation hubs that could better harness emerging technologies being developed across allied capitals. While the Defense Department is focused on initiatives that will improve America’s sclerotic acquisition and innovation processes, these efforts need an alliance-centric approach from inception, rather than treating allies as an add-on to existing American plans. NATO, for example, might consider establishing an allied version of the Defense Advanced Research Projects Agency (DARPA), in which key allies could collaborate on emerging technologies, as proposed by the 2017 GLOBSEC NATO Adaptation Initiative. Indo-Pacific allies such as Australia, Japan, and South Korea could be incorporated in this initiative through their role as NATO “global partners.”

#### NATO leadership and Indo-Pacific allied cooperation on EDT innovation is key to counter China.

Nouwens 22 — Meia Nouwens, Senior Fellow for Chinese Defence Policy and Military Modernisation at the International Institute for Strategic Studies (UK), Co-Leader of the China Security Project at the Mercator Institute for China Studies (Germany), holds an M.A. in International Relations and Diplomacy from Leiden University (Netherlands) and an M.Phil. in Modern Chinese Studies from the University of Oxford (UK) and Peking University (China), 2022 (“NATO and Digital Cooperation with the Indo-Pacific,” German Marshall Fund of the United States, February 11th, Available Online at https://www.gmfus.org/news/nato-and-digital-cooperation-indo-pacific, Accessed 07-07-2022)

Meeting the Challenge: Digital Technologies

Due to the nature of the challenges that China poses to it, NATO’s priority should be to meet them at home. However, in countering the economic, technological, and security challenges that China poses, collaboration with partner countries in the Indo-Pacific that are like-minded and have valuable experience in countering Beijing’s assertiveness is equally important. Nevertheless, as Secretary General Stoltenberg has stated, NATO is unlikely to face the China challenge by being physically present in the South China Sea or elsewhere in the Indo-Pacific region.25 to resource constraints and other concerns, this remains unlikely in the near future. NATO can best meet the technological challenge that China poses through greater collaboration and coordination with regard to the digital space and emerging and disruptive technologies. While current NATO activity in EDTs, as well as in data management and governance, is a step in the right direction to protect domestic resilience and to enhance innovation capacities, there are further options to strengthen the alliance’s technological edge at home and with partners in the Indo-Pacific.

Expand NATO collaboration on EDTs to partners in the Indo-Pacific

NATO is in the process of developing the mechanisms, funding, and strategy behind DIANA and the NATO Innovation fund, the former aimed at launching in 2023 and the latter potentially totaling to $1 billion. DIANA aims to be NATO’s version of the United States’ Defense Advanced Research Projects Agency and to bring together transatlantic efforts on critical technologies, working with industry and academia on AI, big-data processing, quantum-enabled technologies, autonomy, biotechnology, hypersonic weapons, and space. Subsequently, the Innovation Fund will seek initially to invest $81.2 million per year in transatlantic startups. Importantly, it will work with pre-vetted investors to ensure that “the technology will be protected from illicit transfers.”26

While much is still left to be decided on both these efforts, there are clear areas for practical cooperation with partners in the Indo-Pacific; for example, with regard to the Australia-United Kingdom-United States (AUKUS) security pact and the Quadrilateral Security Dialogue joining Australia, India, Japan, and the United States.

First, AUKUS aims to promote cooperation beyond the initially agreed nuclear-powered-submarine program. The agreement seeks to foster “deeper integration of security and defense-related science, technology, industrial bases and supply chains.”27 Trilateral collaboration will focus on cyber capabilities, AI, quantum technologies, and additional undersea capabilities.

Following the first in-person leaders’ summit of the Quad in September 2021, leaders of the four countries put forth an initiative to partner on emerging technologies, space, and cybersecurity, and to cultivate next-generation talent.28 Exact timelines for these initiatives are still unclear. With regard to the latter, the Quad Fellowship will provide 100 scholarships per year for students in science, technology engineering, and mathematics from the four countries to study in the United States. Ultimately, the program will seek to develop a network of science and technology experts among the Quad countries. On critical and emerging technologies, the countries will work together to publish a statement of principles that touches on the design, development, governance, and use of technology; to establish a technical standards contact group; to launch a semiconductor supply-chain initiative; to support 5G deployment and diversification; and to monitor advances in biotechnologies.29 The Quad countries will also collaborate on cybersecurity issues and establish a space-related working group that shares climate change-related satellite data, enables capacity-building in space-related domains in other Indo-Pacific countries, and consults on norms and guidelines.

While the overlap is not exact, there are significant areas for cooperation between NATO, AUKUS, and Quad countries. Australia and Japan are already NATO partner countries and cooperate politically with the alliance on a variety of levels from parliaments to heads of state, ministries of foreign affairs and defense.30 **[[[\*\*\*Start Footnote 30\*\*\*]** NATO’s “global partners,” such as Australia and Japan, are countries with whom the alliance engages politically and have access to the same activities that NATO Individual Partnership Cooperation Programme countries receive. They work with NATO on areas of common interest, such as cyber defence, counterterrorism, non-proliferation, and resilience. In some cases, NATO and its global partners cooperate through NATO military operations or through defence capacity, training, and educational programmes. See NATO, Relations with partners across the globe, August 25, 2021. **[[[\*\*\*End Footnote 30\*\*\*]]]** Bringing partner countries into NATO’s programing on EDTs would not only increase the alliance’s innovative capacities but also allow it to align itself with the priorities of partners in the Indo-Pacific to a greater extent.

A potential stumbling block for such cooperation might be the recent tensions between the EU (and therefore some NATO members) and the AUKUS countries. Transatlantic relations soured following the announcement of the establishment of the security pact and the related cancellation of the submarine deal worth $90 billion between Australia and France. The announcement of AUKUS also coincided with the publication of the EU’s Indo-Pacific strategy, which highlights the ambition to work with the Quad in the region.31 There is thus a potential risk that EU members that are also NATO members, in particular France, may prioritize technological development within an EU rather than NATO context.

This risk may be overstated, however. The EU’s Indo-Pacific strategy focuses primarily on digital governance and partnerships: the development of shared technological standards, alone and together in coordination with like-minded partners, for areas such enhancing governance around AI based on democratic principles and fundamental rights. The EU’s practical engagement with its Indo-Pacific partners on the development of EDTs is still limited. It only has agreements on areas of practical cooperation and development with a select few countries in the Indo-Pacific, such as India and Japan with which it has agreed to deepen cooperation on 6G, standardization, AI, blockchain, and quantum and other technologies.

Second, the security and defense section of the EU’s Indo-Pacific strategy does not make any mention of cooperation with like-minded countries in the Indo-Pacific on EDTs. The strategy’s main focus here is on cooperation on disinformation, maritime security, outer space, cybersecurity, peacekeeping, counterterrorism, and arms control. As the EU’s focus on EDTs is primarily on standard setting, governance, ethics, and civilian applications, there may be an opportunity to collaborate and share the burden with NATO. NATO could work alongside the EU to ensure standards are set for EDTs in the defense and civilian realms while taking the lead on the development and adoption of defense-related EDTs.

Establish NATO standards on data governance together with partners in the Indo-Pacific

In 2017, the commander of NATO’s Allied Command for Transformation, General Denis Mercier, stated that “data is now a main strategic resource. Processes for collecting, sharing, exploiting and distributing data are the main drivers to adapting organizations.”32 This remains true with regard to the military and civilian, public and private sectors. If shared policies on data governance promote interoperability, help to establish rules and norms, and secure data, then divergent policies could have the opposite effect. If NATO aims to remain competitive and to increase its innovation strengths in EDTs and digital technologies, digital policy coordination should be an area of discussion within the alliance.

In October 2021, NATO defense ministers agreed to the alliance’s first-ever strategy for AI, which includes an ambition to agree on standards of data collection and use for AI. NATO also has standards and processes related to big data produced by the alliance.33 However, if NATO members and partner countries seek to cooperate and collaborate on the development and adoption of emerging technologies and data-driven innovation, then addressing data governance and trusted cross-border data flows between allies and across partners is of importance. To date, some NATO members are aligned through membership of the EU and its General Data Protection Regulation (GDPR) and through the European Data Governance Act (subject to final approval by the European Parliament and Council of the EU this year).34 However, other allies, such as the United States, have taken different approaches to data governance and it remains to be seen whether the new EU-US Trade and Technology Council can find solutions for transatlantic cooperation in this area.35

Last, if collaboration between the innovative economies of NATO allies and their partners in the Indo-Pacific is a goal, then greater like-mindedness and alignment of data-governance norms should be an area of consideration in the future within the alliance and with countries like Australia, India, and Japan.

This undoubtedly falls outside of the realm of NATO’s traditional area of competence and more clearly a suitable role for the European Commission. This is not an obstacle: NATO has agreed already to work with the EU in areas where the latter has experience and competence. Furthermore, the EU is an active player in bilateral discussions between member states and non-EU countries about data sharing and data governance. Its Indo-Pacific strategy already envisions a greater role for the EU in the region in areas of digital governance through Digital Partnership Agreements with Japan, Singapore, and South Korea. The EU has already deepened its digital partnership with India in 2021 which seeks to promote 5G in line with global strategies and develop joint visions for next generations of information and communications technology, to promote digital cooperation between private sectors in each country, and to ensure that data regulation in India and the EU align with each other. Similarly, the EU and Japan created the world’s largest area of safe data flows in 2019 when the European Commission adopted an adequacy decision on Japan for a data-sharing agreement.36

Conclusion

While countering the challenges that China poses to NATO will not be easy, the greatest challenge will be to find agreement and unity between allies on how to address their shared concerns about China’s rise. The limitations on NATO’s resources, particularly due to the requirements of allies to focus on collective security and defense at home, will make it difficult for the alliance to counter the China challenge in the Indo-Pacific. Though a show of commitment by sending military assets to the region and NATO’s partners there is important, addressing the challenges that China poses to the alliance and its partners alike should be done in more varied ways.

NATO should focus on expanding its current work in the digital sphere to cooperation and collaboration with partner countries in the Indo-Pacific in order to build a strong ecosystem of like-minded digital actors. By cooperating on EDTs and sharing data to ensure that the private and public sectors in allied and partner countries as well as institutions like the EU remain competitive, NATO and like-minded countries can take steps toward bolstering their defense and security capabilities and preparing for competition as well as for conflict.

#### Failing to effectively counter China causes war — we’re on the brink.

Colby 22 — Elbridge Colby, Co-Founder and Principal of The Marathon Institute—a policy initiative focused on developing strategies to prepare the United States for an era of sustained great power competition, Member of the Council on Foreign Relations, former Director of the Defense Program at the Center for a New American Security, former Deputy Assistant Secretary of Defense for Strategy and Force Development at the U.S. Department of Defense, Recipient of the Distinguished and Exceptional Public Service Awards from the U.S. Department of Defense and of the Superior and Meritorious Honor Awards from the U.S. Department of State, holds a J.D. from Yale Law School, 2022 (“China, Not Russia, Still Poses the Greatest Challenge to U.S. Security,” *The National Interest*, July 1st, Available Online at https://nationalinterest.org/feature/china-not-russia-still-poses-greatest-challenge-us-security-203228, Accessed 07-12-2022)

American foreign policy after—indeed, during—the Russo-Ukrainian War should promptly head to the world’s most decisive region: Asia. This will require that American foreign and defense policy genuinely put Asia first—in our military investments, in our allocation of political capital and resources, and in our leaders’ attention.

Nothing that has happened since Russia’s abominable invasion of Ukraine has changed a set of facts: Asia is the world’s largest market area, and it is growing in global share. Located in the middle of Asia is China which, alongside the United States, is one of the world’s two superpowers. China’s behavior has become increasingly aggressive and domineering and appears oriented toward establishing Beijing’s hegemony over Asia. If Beijing achieves this goal, the resulting consequences for American life will be dire.

Preventing China from establishing this hegemony over Asia must therefore be the priority of U.S. foreign policy—even in the face of what is happening in Europe. The simple fact is that Asia is more important than Europe, and China is a much greater threat than Russia. By way of comparison, Asia’s economy is roughly twice as large as Europe’s today—but within twenty years it will likely be multiple times greater. China, in the meantime, has a GDP roughly an order of magnitude larger than Russia’s.

If current trends continue, China appears on a trajectory to achieve its hegemonic ambitions. Beijing has been building a military distinctly not limited to territorial defense. Rather, it will be capable of enabling Beijing’s pursuit of much larger and ambitious goals—first by ingesting Taiwan, but not ending there. Indeed, amidst the furor over the war in Ukraine, Beijing announced yet again that it would increase its defense spending by 7 percent this year. Meanwhile, despite much talk, the United States has neglected its military position in Asia, while many of its allies—especially Japan and Taiwan—have been laggard in maintaining their defenses. As a result, the military balance in Asia has continued to shift markedly against the United States and our allies. In blunt terms, we are now rapidly approaching, if not already in, the window of opportunity where China might well decide to attack Taiwan—and we might lose.

Avoiding this outcome must be the top, overriding priority for U.S. policy. This does not mean Europe is unimportant or that we should neglect or abandon it. We should actively support Ukraine with weapons and other forms of support while remaining firmly committed to NATO, albeit with our contributions being more focused and narrow in scale. But it does mean Asia must be our priority, and genuinely so, not just rhetorically as has so often been the case in the past.

Because of these factors, shifting our focus to Asia would make sense regardless of how Russia’s invasion of Ukraine fared. But, if anything, the war in Ukraine and the reaction to it has made it even more palatable for the United States to turn to Asia. Moscow, while still menacing and dangerous, has vividly demonstrated that its power is less formidable than many of us had feared. Russia is very likely to try to recover its strength, but the losses of war and the impact of sanctions are likely to make that process slow and difficult. At the same time, Europe has stood up, announcing major increases in defense spending, supporting Ukraine’s own self-defense, and demonstrating an unprecedented degree of cohesion in applying sanctions and other forms of pressure on Russia.

The result is that Moscow appears less of a threat than many of us had supposed, while Europeans are doing more to shoulder their own defense. If anything, this should make the United States more, not less, ready to focus on Asia. Indeed, in these circumstances, it is actually hard to understand the logic of increasing America’s focus on Europe. Why would we double down in Europe at the expense of Asia when there is less of a threat from Russia and more European self-help—all while the danger in the primary theater only increases?

Yet many in the foreign policy and political elite seem to view the Russo-Ukrainian War as an opportunity precisely to double down in Europe. Even more, for some, it is a chance to try to turn the foreign policy clock back to the globe-spanning liberal imperialism of two decades ago.

Washington must resist this temptation like the plague. The breathtakingly hubristic foreign policies of the 2000s were unwise even in the period of unipolarity, as we have found to our chagrin. As American leaders sermonized on an end to evil, China rose at our expense; our military expeditions in the Middle East ended in frustration, when not failure; and we lost our military edge and many of our economic advantages. But such policies would be even more extraordinarily ill-advised when we are now locked in a strategic rivalry with a superpower China that is far more powerful than the USSR, Germany, or Japan ever were. We simply do not have the preponderance of power to waste our resources anymore.

Time, then, to focus on the region and the contest that really matters: the effort to deny China’s dominance of Asia. We are already well behind in that struggle, and every day we neglect to increase our focus further increases the chances of crisis, war, and defeat—with grievous consequences for all Americans.

#### Strengthening allied power to counter China is the only way to prevent great power war — accommodation makes it inevitable.

Beckley 22 — Michael Beckley, Associate Professor of Political Science at Tufts University, Nonresident Senior Fellow at the American Enterprise Institute, former Senior China Policy Analyst at the Science Applications International Corporation—a government services and IT support company, former Faculty Fellow in National Security in the Office of the Secretary of Defense for Policy Planning at the U.S. Department of Defense, holds a Ph.D. in Political Science from Columbia University, former policy debater at College Prep and Emory University, 2022 (“Enemies of My Enemy: How Fear of China Is Forging a New World Order,” *Foreign Affairs*, March/April, Available Online at https://www.foreignaffairs.com/articles/2021-02-14/china-new-world-order-enemies-my-enemy, Accessed 07-07-2022)

The Clash of Systems

The history of international order building is one of savage competition between clashing systems, not of harmonious cooperation. In the best of times, that competition took the form of a cold war, with each side jockeying for advantage and probing each other with every measure short of military force. In many cases, however, the competition eventually boiled over into a shooting war and ended with one side crushing the other. The victorious order then ruled until it was destroyed by a new competitor—or until it simply crumbled without an external threat to hold it together.

Today, a growing number of policymakers and pundits are calling for a new concert of powers to sort out the world’s problems and divide the globe into spheres of influence. But the idea of an inclusive order in which no one power’s vision prevails is a fantasy that can exist only in the imaginations of world-government idealists and academic theorists. There are only two orders under construction right now—a Chinese-led one and a U.S.-led one—and the contest between the two is rapidly becoming a clash between autocracy and democracy, as both countries define themselves against each other and try to infuse their respective coalitions with ideological purpose. China is positioning itself as the world’s defender of hierarchy and tradition against a decadent and disorderly West; the United States is belatedly summoning a new alliance to check Chinese power and make the world safe for democracy.

This clash of systems will define the twenty-first century and divide the world. China will view the emerging democratic order as a containment strategy designed to strangle its economy and topple its regime. In response, it will seek to protect itself by asserting greater military control over its vital sea-lanes, carving out exclusive economic zones for its firms, and propping up autocratic allies as it sows chaos in democracies. The upsurge of Chinese repression and aggression, in turn, will further impel the United States and its allies to shun Beijing and build a democratic order. For a tiny glimpse of what this vicious cycle might look like, consider what happened in March 2021, when Canada, the United Kingdom, the United States, and the EU sanctioned four Chinese officials for human rights abuses in Xinjiang. The sanctions amounted to a slap on the wrist, but Beijing interpreted them as an assault on its sovereignty and unleashed a diplomatic tirade and a slew of economic sanctions. The EU returned fire by freezing its proposed EU-China Comprehensive Agreement on Investment.

In the coming years, the trade and technology wars between China and the United States that began during the Trump administration will rage on as both sides try to expand their respective spheres. Other countries will find it increasingly difficult to hedge their bets by maintaining links to both blocs. Instead, China and the United States will push their partners to pick sides, compelling them to reroute their supply chains and adopt wholesale the ecosystem of technologies and standards of one side’s order. The Internet will be split in two. When people journey from one order to the other—if they can even get a visa—they will enter a different digital realm. Their phones won’t work, nor will their favorite websites, their email accounts, or their precious social media apps. Political warfare between the two systems will intensify, as each tries to undermine the domestic legitimacy and international appeal of its competitor. East Asian sea-lanes will grow clogged with warships, and rival forces will experience frequent close encounters.

The standoff will end only when one side defeats or exhausts the other. As of now, the smart money is on the U.S. side, which has far more wealth and military assets than China does and better prospects for future growth. By the early 2030s, Xi, an obese smoker with a stressful job, will be in his 80s, if he is still alive. China’s demographic crisis will be kicking into high gear, with the country projected to lose roughly 70 million working-age adults and gain 130 million senior citizens between now and then. Hundreds of billions of dollars in overseas Chinese loans will be due, and many of China’s foreign partners won’t be able to pay them back. It is hard to see how a country facing so many challenges could long sustain its own international order, especially in the face of determined opposition from the world’s wealthiest countries.

Yet it is also far from guaranteed that the U.S.-led democratic order will hold together. The United States could suffer a constitutional crisis in the 2024 presidential election and collapse into civil strife. Even if that doesn’t happen, the United States and its allies might be rent by their own divides. The democratic world is suffering its greatest crisis of confidence and unity since the 1930s. Nationalism, populism, and opposition to globalism are rising, making collective action difficult. The East Asian democracies have ongoing territorial disputes with one another. Many Europeans view China as more of an economic opportunity than a strategic threat and seriously doubt the United States’ reliability as an ally, having endured four years of tariffs and scorn from President Donald Trump, who could soon be back in power. Europeans also hold different views from Americans on data security and privacy, and European governments fear U.S. technology dominance almost as much as they do Chinese digital hegemony. India may not be ready to abandon its traditional policy of nonalignment and back a democratic order, especially when it is becoming more repressive at home, and an order built around democracy will struggle to form productive partnerships with autocracies that would be important partners in any alliance against China, such as Singapore and Vietnam. Fear of China is a powerful force, but it might not be potent enough to paper over the many cracks that exist within the emerging anti-Chinese coalition.

If that coalition fails to solidify its international order, then the world will steadily slide back into anarchy, a struggle among rogue powers and regional blocs in which the strong do what they can and the weak suffer what they must. Some scholars assume—or hope—that an unordered world will sort itself out on its own, that great powers will carve out stable spheres of influence and avoid conflict or that the spread of international commerce and enlightened ideas will naturally maintain global peace and prosperity. But peace and prosperity are unnatural. When achieved, they are the result of sustained cooperation among great powers—that is, of an international order.

Doubling Down On Democracy

History shows that eras of fluid multipolarity typically end in disaster, regardless of the bright ideas or advanced technologies circulating at the time. The late eighteenth century witnessed the pinnacle of the Enlightenment in Europe, before the continent descended into the hell of the Napoleonic Wars. At the start of the twentieth century, the world’s sharpest minds predicted an end to great-power conflict as railways, telegraph cables, and steamships linked countries closer together. The worst war in history up to that point quickly followed. The sad and paradoxical reality is that international orders are vital to avert chaos, yet they typically emerge only during periods of great-power rivalry. Competing with China will be fraught with risk for the United States and its allies, but it might be the only way to avoid even greater dangers.

To build a better future, the United States and its allies will need to take a more enlightened view of their interests than they did even during the Cold War. Back then, their economic interests dovetailed nicely with their geopolitical interests. Simple greed, if nothing else, could compel capitalist states to band together to protect private property against a communist onslaught. Now, however, the choice is not so simple, because standing up to China will entail significant economic costs, especially in the short term. Those costs might pale in comparison to the long-term costs of business as usual with Beijing—Chinese espionage has been estimated to deprive the United States alone of somewhere between $200 billion and $600 billion annually—to say nothing of the moral quandaries and geopolitical risks of cooperating with a brutal totalitarian regime with revanchist ambitions. Yet the ability to make such an enlightened calculation in favor of confronting China may be beyond the capacities of any nation, especially ones as polarized as the United States and many of its democratic allies.

If there is any hope, it lies in a renewed commitment to democratic values. The United States and its allies share a common aspiration for an international order based on democratic principles and enshrined in international agreements and laws. The core of such an order is being forged in the crucible of competition with China and could be built out into the most enlightened order the world has ever seen—a genuine free world. But to get there, the United States and its allies will have to embrace competition with China and march forward together through another long twilight struggle.

#### Nuclear escalation is likely — urgently strengthening allied coordination to send a signal of resolve is the only way to prevent it.

Pettyjohn and Wasser 22 — Stacie L. Pettyjohn, Senior Fellow and Director of the Defense Program at the Center for a New American Security, Adjunct Professor in the School of Advanced International Studies at Johns Hopkins University, former Senior Political Scientist and Director of the Strategy and Doctrine Program of Project AIR FORCE at the RAND Corporation, holds a Ph.D. in Foreign Affairs from the University of Virginia, and Becca Wasser, Fellow in the Defense Program and Co-Leader of The Gaming Lab at the Center for a New American Security, Adjunct Instructor in the School of Foreign Service at Georgetown University, former Senior Policy Analyst at the RAND Corporation, former Program Officer and Research Analyst at the International Institute for Strategic Studies (UK), holds an M.S. in Foreign Service from Georgetown University, 2022 (“A Fight Over Taiwan Could Go Nuclear: War-Gaming Reveals How a U.S.-Chinese Conflict Might Escalate,” *Foreign Affairs*, May 20th, Available Online at https://www.foreignaffairs.com/articles/china/2022-05-20/fight-over-taiwan-could-go-nuclear, Accessed 07-12-2022)

Russia’s invasion of Ukraine has raised the specter of nuclear war, as Russian President Vladimir Putin has placed his nuclear forces at an elevated state of alert and has warned that any effort by outside parties to interfere in the war would result in “consequences you have never seen.” Such saber-rattling has understandably made headlines and drawn notice in Washington. But if China attempted to forcibly invade Taiwan and the United States came to Taipei’s aid, the threat of escalation could outstrip even the current nerve-wracking situation in Europe.

A recent war game, conducted by the Center for a New American Security in conjunction with the NBC program “Meet the Press,” demonstrated just how quickly such a conflict could escalate. The game posited a fictional crisis set in 2027, with the aim of examining how the United States and China might act under a certain set of conditions. The game demonstrated that China’s military modernization and expansion of its nuclear arsenal—not to mention the importance Beijing places on unification with Taiwan—mean that, in the real world, a fight between China and the United States could very well go nuclear.

Beijing views Taiwan as a breakaway republic. If the Chinese Communist Party decides to invade the island, its leaders may not be able to accept failure without seriously harming the regime’s legitimacy. Thus, the CCP might be willing to take significant risks to ensure that the conflict ends on terms that it finds acceptable. That would mean convincing the United States and its allies that the costs of defending Taiwan are so high that it is not worth contesting the invasion. While China has several ways to achieve that goal, from Beijing’s perspective, using nuclear weapons may be the most effective means to keep the United States out of the conflict.

Gearing For Battle

China is several decades into transforming its People’s Liberation Army (PLA) into what the Chinese President Xi Jinping has called a “world-class military” that could defeat any third party that comes to Taiwan’s defense. China’s warfighting strategy, known as “anti-access/area denial,” rests on being able to project conventional military power out several thousand miles in order to prevent the American military, in particular, from effectively countering a Chinese attack on Taiwan. Meanwhile, a growing nuclear arsenal provides Beijing with coercive leverage as well as potentially new warfighting capabilities, which could increase the risks of war and escalation.

China has historically possessed only a few hundred ground-based nuclear weapons. But last year, nuclear scholars at the James Martin Center for Nonproliferation Studies and the Federation of American Scientists identified three missile silo fields under construction in the Xinjiang region. The Financial Times reported that China might have carried out tests of hypersonic gliders as a part of an orbital bombardment system that could evade missile defenses and deliver nuclear weapons to targets in the continental United States. The U.S. Department of Defense projects that by 2030, China will have around 1,000 deliverable warheads—more than triple the number it currently possesses. Based on these projections, Chinese leaders may believe that as early as five years from now the PLA will have made enough conventional and nuclear gains that it could fight and win a war to unify with Taiwan.

Our recent war game—in which members of Congress, former government officials, and subject matter experts assumed the roles of senior national security decision makers in China and the United States—illustrated that a U.S.-Chinese war could escalate quickly. For one thing, it showed that both countries would face operational incentives to strike military forces on the other’s territory. In the game, such strikes were intended to be calibrated to avoid escalation; both sides tried to walk a fine line by attacking only military targets. But such attacks crossed red lines for both countries, and produced a tit-for-tat cycle of attacks that broadened the scope and intensity of the conflict.

For instance, in the simulation, China launched a preemptive attack against key U.S. bases in the Indo-Pacific region. The attacks targeted Guam, in particular, because it is a forward operating base critical to U.S. military operations in Asia, and because since it is a territory, and not a U.S. state, the Chinese team viewed striking it as less escalatory than attacking other possible targets. In response, the United States targeted Chinese military ships in ports and surrounding facilities, but refrained from other attacks on the Chinese mainland. Nevertheless, both sides perceived these strikes as attacks on their home territory, crossing an important threshold. Instead of mirror-imaging their own concerns about attacks on their territory, each side justified the initial blows as military necessities that were limited in nature and would be seen by the other as such. Responses to the initial strikes only escalated things further as the U.S. team responded to China’s moves by hitting targets in mainland China, and the Chinese team responded to Washington’s strikes by attacking sites in Hawaii.

A New Era

One particularly alarming finding from the war game is that China found it necessary to threaten to go nuclear from the start in order to ward off outside support for Taiwan. This threat was repeated throughout the game, particularly after mainland China had been attacked. At times, efforts to erode Washington’s will so that it would back down from the fight received greater attention by the China team than the invasion of Taiwan itself. But China had difficulty convincing the United States that its nuclear threats were credible. In real life, China’s significant and recent changes to its nuclear posture and readiness may impact other nations’ views, as its nuclear threats may not be viewed as credible given its stated doctrine of no first use, its smaller but burgeoning nuclear arsenal, and lack of experience making nuclear threats. This may push China to preemptively detonate a nuclear weapon to reinforce the credibility of its warning.

China might also resort to a demonstration of its nuclear might because of constraints on its long-range conventional strike capabilities. Five years from now, the PLA still will have a very limited ability to launch conventional attacks beyond locations in the “second island chain” in the Pacific; namely, Guam and Palau. Unable to strike the U.S. homeland with conventional weapons, China would struggle to impose costs on the American people. Up until a certain point in the game, the U.S. team felt its larger nuclear arsenal was sufficient to deter escalation and did not fully appreciate the seriousness of China’s threats. As a result, China felt it needed to escalate significantly to send a message that the U.S. homeland could be at risk if Washington did not back down. Despite China’s stated “no-first use” nuclear policy, the war game resulted in Beijing detonating a nuclear weapon off the coast of Hawaii as a demonstration. The attack caused relatively little destruction, as the electromagnetic pulse only damaged the electronics of ships in the immediate vicinity but did not directly impact the U.S. state. The war game ended before the U.S. team could respond, but it is likely that the first use of a nuclear weapon since World War II would have provoked a response.

The most likely paths to nuclear escalation in a fight between the United States and China are different from those that were most likely during the Cold War. The Soviet Union and the United States feared a massive, bolt-from-the-blue nuclear attack, which would precipitate a full-scale strategic exchange. In a confrontation over Taiwan, however, Beijing could employ nuclear weapons in a more limited way to signal resolve or to improve its chances of winning on the battlefield. It is unclear how a war would proceed after that kind of limited nuclear use and whether the United States could de-escalate the situation while still achieving its objectives.

An Ounce of Prevention

The clear lesson from the war game is that the United States needs to strengthen its conventional capabilities in the Indo-Pacific to ensure that China never views an invasion of Taiwan as a prudent tactical move. To do so, the United States will need to commit to maintaining its conventional military superiority by expanding its stockpiles of long-range munitions and investing in undersea capabilities. Washington must also be able to conduct offensive operations inside the first and second island chains even while under attack. This will require access to new bases to distribute U.S. forces, enhance their survivability, and ensure that they can effectively defend Taiwan in the face of China’s attacks.

Moreover, the United States needs to develop an integrated network of partners willing to contribute to Taiwan’s defense. Allies are an asymmetric advantage: the United States has them, and China does not. The United States should deepen strategic and operational planning with key partners to send a strong signal of resolve to China. As part of these planning efforts, the United States and its allies will need to develop war-winning military strategies that do not cross Chinese red-lines. The game highlighted just how difficult this task may be; what it did not highlight is the complexity of developing military strategies that integrate the strategic objectives and military capacities of multiple nations.

Moving forward, military planners in the United States and in Washington’s allies and partners must grapple with the fact that, in a conflict over Taiwan, China would consider all conventional and nuclear options to be on the table. And the United States is running out of time to strengthen deterrence and keep China from believing an invasion of Taiwan could be successful. The biggest risk is that Washington and its friends choose not to seize the moment and act: a year or two from now, it might already be too late.

## Case Backlines

### They Say: “Status Quo Solves”

#### This arg takes out their disads, not our case — NATO has already committed to increase EDT innovation, but the missing piece remains increased U.S. security cooperation. That’s the plan.

Christie 22 — Edward Hunter Christie, Senior Research Fellow at the Finnish Institute of International Affairs (Finland), Senior Fellow at the Prague Security Studies Institute (Czechia), Research Associate at the Wilfried Martens Centre for European Studies (Germany), Doctoral Fellow at Vrije Universiteit Brussel (Belgium), Founder of AI Policy Consulting (Belgium), former Deputy Head of the Innovation Unit at NATO, holds an M.Sc. in Economics from the London School of Economics and Political Science (UK), 2022 (“Defence cooperation in artificial intelligence: Bridging the transatlantic gap for a stronger Europe,” *European View*, Volume 21, Issue 1, Available Online at https://journals.sagepub.com/doi/pdf/10.1177/17816858221089372, Accessed 07-17-2022, p. 17-19)

Investment challenges

As noted in the introduction, there is a significant gap between overall US and European defence spending levels. This general pattern also holds for defence research and development spending. In 2020, EU spending in this area amounted to €8 billion (EDA 2021). For the US, with caveats as to comparability, expenditure for ‘research, development, test and evaluation’ totalled approximately €90 billion3 in the 2021 fiscal year (from October 2020 to September 2021), or about 10 times more.

Investment challenges go beyond issues of scale. The US also has greater experience in the setting up and operation of structures to promote both military and dual-use innovation. While the best-known institution is the Defense Advanced Research Projects Agency, other US government structures are also relevant in discussions on fostering innovation in AI for military applications. A much-discussed example is In-Q-Tel, which was originally set up as the state venture-capital arm of the Central Intelligence Agency. To illustrate the influence of the In-Q-Tel example, one may note that both its current Chief Executive Officer, Chris Darby, and one of its former Chief Executive Officers, Gilman Louie, served among the 15 commissioners of the National Security Commission on Artificial Intelligence.4 This was a temporarily created expert commission mandated [end page 17] by the US Congress to provide policy recommendations for a whole-of-government and whole-of-society approach for US AI policy.5

With In-Q-Tel, the idea is to learn from private-sector practices in the area of venture-capital investment and repurpose them for state needs and more patient time horizons. A supported company should pursue product development strategies aimed at serving both civilian markets and government needs. In this way, rather than effectively taking over a commercial company and limiting its growth potential to future government contracts alone, the government body encourages an intermediate trajectory made up of mixed revenue streams, in the hope that this will generate greater returns to scale and higher efficiency thanks to the disciplining effect of private-sector competition. Conversely, the advantage of this approach as compared to not intervening at all is that the commercial company will integrate current and likely future government needs into its product and business-development strategy, rather than ignoring them and finding itself, at a later date, unable to supply the government sector according to the latter’s requirements.

A related issue which falls between what can be achieved with new investment instruments and new protections that can be assured through the screening of foreign direct investment is the provision of investment from trusted private investors to the technology sector. Certain technology companies that are not part of the traditional defence industry may be developing dual-use products that are of potential interest to the defence sector while having limited awareness of national security concerns. This may make them vulnerable targets for both licit and illicit attempts to acquire their technologies on the part of foreign state actors. At the same time, their business development needs may lead them to seek investment from any potential source, thus exposing them to potential risks. To respond to this challenge, the US Department of Defense has launched a scheme called the Trusted Capital Marketplace (US Department of Defense 2021a).

Building on these considerations, the NATO Innovation Unit has developed two new instruments for Allied use which were announced to the public in October 2021 (NATO 2021a; 2021b). Both instruments aim to foster technological innovation with a deliberate focus on dual-use applications and on enterprises with mixed (potential) revenue streams. The first instrument is the Defence Innovation Accelerator for the North Atlantic (DIANA), which is a NATO instrument, that is, it involves the participation of all 30 NATO Allies. The second instrument is the NATO Innovation Fund, which in NATO terminology is a ‘multinational’ instrument, namely one that Allies freely opt into.

DIANA will aim to accelerate the adoption of dual-use technological solutions through several interlocking components.6 First, it will develop a network of national organisations, in particular test centres and innovation accelerators. Second, it will competitively select private-sector innovators and allow them to use national organisations in the network to interface with military end users and military capability-development specialists. Third, it is envisaged that DIANA will provide mentorship and education services for private innovators to familiarise them with the opportunities and responsibilities inherent to the defence and security sector. Fourth, DIANA will develop a database of trusted financial investors from Allied nations and support matchmaking between investors and innovators. Fifth and [end page 18] finally, DIANA will also provide expert advice on defence and security innovation to all relevant stakeholders, including private-sector and academic entities.

Regarding the NATO Innovation Fund, 17 Allies had opted into the Fund as of the date of its announcement in October 2021. The participating Allies will inject up to €1 billion into Allied innovation ecosystems over the next 15 years. The Fund aims to attract additional private investments due to the de-risking effect, both financial and technological, thanks to state co-funding and diligence and screening efforts. The funds are intended to be used for long-term support of ‘deep tech’ innovative companies, that is, for advanced research into AI, quantum and related technologies that may have both military and civilian applications. Due diligence and security screening practices will aim to ensure that both private investors and fund recipients are trusted entities.

Conclusions

Much has already been achieved in terms of new structures, new initiatives and new policy developments to support the collaborative adoption of AI among NATO Allies and EU member states. In addition to pre-existing structures and mechanisms at both the NATO and EU levels, which have ensured that nations are not starting from scratch, national defence institutions are already able to refer to common policy commitments and to options, whether through NATO or the EDA, for research or capability-development activities. At the same time, ensuring a competitive edge in AI is a truly whole-of-government effort which requires considerable cross-over between the military and civilian realms.

Large gaps remain between the US and the EU on certain key indicators. At the same time, the gaps pertaining to research are far smaller. To ensure greater European performance and relevance in AI in general, and its defence applications in particular, it seems desirable to focus on two strategic priorities: investment volumes, both public and private, which need to be significantly increased; and the full use of collaborative mechanisms involving the US.

To that end, it would be beneficial for nations on both sides of the Atlantic to ensure that a clear and common vision is set out in forthcoming strategic documents, most notably the EU’s Strategic Compass and NATO’s new Strategic Concept. This should include clear political commitments to increasing investment, both in general and in instruments for promoting collaborative innovation. There are opportunities for ‘more Europe’ through the EDA and the European Defence Fund. But while pursuing those avenues, European capitals should prioritise efforts that complement and enhance transatlantic approaches, in recognition of the reality that the US remains the indispensable ally for Europe’s security.

#### Status quo not sufficient.

Grabar-Kitarović 22 — Kolinda Grabar-Kitarović, Member of the Advisory Committee of the Future Security and Defence Council at GLOBSEC—a think tank in Slovakia, former President of Croatia (from 2015 to 2020), former NATO Assistant Secretary-General for Public Diplomacy, former Croatian Ambassador to the United States, holds an M.A. in International Relations from the University of Zagreb (Croatia), 2022 (“NATO Must Ensure Defense and Civilian Industries Work Together,” *Defense One*, June 16th, Available Online at https://www.defenseone.com/ideas/2022/06/nato-must-ensure-defense-and-civilian-industries-work-together/368250/, Accessed 07-03-2022)

The internet, microwaves, and synthetic rubber came into our lives as products invented for military purposes. Even everyday things, such as undershirts and concentrated fruit juice were created to improve the combat readiness of armed forces. Though many people typically associate the military with war and suffering, this industry has been a source of incredible progress, producing inventions that made our lives longer, healthier, and easier. These days, innovation is likely to run the other way, with the military benefiting from inventions developed with private funding.

A symbiotic relationship between military needs and human progress is not necessarily the default. Instead, it requires a well-oiled innovation ecosystem in which military and civilian industries share their expertise and knowledge with one another. NATO has recently announced several initiatives to build on past success, but more are needed—particularly as members increase their military funding.

Virtually all alliance members are investing more in defense or are soon planning to do so. Germany, for example, declared that it would create a 100-billion-Euro fund and reach its 2% goal in 2022. Poland, which shares the longest EU border with Ukraine, has taken in more than 3.5 million Ukrainian refugees and promised to dedicate 3% of its GDP to defense. Croatia ramped up its defense investment to 2.3% of GDP.

To ensure that this new investment spurs innovation and co-operation between military and civilian industries as well as academia, NATO announced in April the Defense Innovation Accelerator for the North Atlantic. DIANA will concentrate on deep technologies, including artificial intelligence, big-data processing, quantum-enabled technologies, biotechnology, novel materials, and outer space. In addition, 17 NATO nations have agreed to set up the world’s first multi-sovereign venture capital fund. It will invest 1 billion Euros in early-stage startups and other deep tech funds aligned with its strategic objectives.

But NATO members need to do more to maintain their technological advantage over Russia and China, who are also increasing spending on military research and development. The trends make this clear. In 1960, the U.S. accounted for 69 percent of global R&D investments, with U.S. defense-related R&D accounting for no less than 36% of global spending. The bulk (65%) of U.S. investments in defense-related R&D was financed from the federal budget. However, by 2019, the U.S. share of global R&D fell to 30%, and the share of federal government investment in defense-related R&D fell from 65% to 21%, whereas the share of business investment in R&D has grown from 33% to 71%. This leaves no doubt that meaningful innovation is not possible without close co-operation with the private sector.

As NATO prepares to adopt its next Strategic Concept at the summit in Madrid, it is essential that it focus on mechanisms that maintain its technological advantage. As part of GLOBSEC’s work at the Future Security and Defense Council, we have proposed several ideas to help promote innovation in the Alliance. We are convinced that NATO’s innovation ecosystem must integrate public and private sectors to ensure this edge.

#### Status quo DIANA and NIF are not sufficient.

Shea and Williams 21 — Jamie Shea, President of the Centre for War Studies at the University of Southern Denmark, former Deputy Assistant Secretary General for Emerging Security Challenges at NATO, holds a D.Phil. in Modern History from Lincoln College, University of Oxford (UK), and Michael John Williams, Associate Professor of International Affairs and Director of the International Relations Program at Syracuse University, Nonresident Senior Fellow with the Transatlantic Security Initiative at the Scowcroft Center for Strategy and Security at The Atlantic Council, Fellow of the Global Diplomacy Lab hosted by the German Foreign Ministry, holds a Ph.D. from the London School of Economics and Political Science, 2021 (“The secret to NATO’s survival: Get political,” *New Atlanticist*—an Atlantic Council blog, June 17th, Available Online at https://www.atlanticcouncil.org/blogs/new-atlanticist/the-secret-to-natos-survival-get-political/, Accessed 07-17-2022)

6. Tackling tech challenges

As Americans memorialized their dead and sat down for barbecues with family and friends over Memorial Day weekend, little did they know that one of the country’s largest meat producers was being hacked with ransomware. The matter hit home again when summer travel plans were upended for thousands as the Steamship Authority in Massachusetts succumbed to a cyberattack. Such attacks against public and private entities will only become more common, and NATO needs to be the forum where transatlantic strategy on tech sovereignty and innovation occurs. What norms and standards are required for a stable and productive future? The focus needs to be not just on disruptive technologies (and resilience, see above), but also on how to open US and European defense markets to foster multinational cooperation in research and development and to develop industry partnerships. The announcements in the summit communiqué on establishing a Defence Innovation Accelerator for the North Atlantic and a NATO Innovation Fund are welcome developments, but more is needed. NATO needs to be the forum where a doctrine of cyber responsibility is developed and deployed.

## AT: CPs (General)

### 2AC — NATO Emerging Tech Key

#### NATO Emerging Tech Key — it’s the foundation of its effectiveness and solves a long list of impacts. This turns their DA impact(s)…

Korb and Cimbala 22 — Lawrence J. Korb, Senior Fellow at the Center for American Progress, Adjunct Professor at Georgetown University, former Senior Fellow and Director of National Security Studies at the Council on Foreign Relations, former Director of the Center for Public Policy Education and Senior Fellow in Foreign Policy Studies at the Brookings Institution, former Assistant U.S. Secretary of Defense (from 1981 to 1985), holds a Ph.D. in Political Science from the State University of New York at Albany, and Stephen J. Cimbala, Distinguished Professor of Political Science at Pennsylvania State University at Brandywine, holds a Ph.D. in Political Science from the University of Wisconsin-Madison, 2022 (“How NATO Can Meet the Challenges of the Twenty-First Century,” *The National Interest*, June 7th, Available Online at https://nationalinterest.org/feature/how-nato-can-meet-challenges-twenty-first-century-202852, Accessed 07-10-2022)

Russian president Vladimir Putin’s February attack on Ukraine was a strategic blunder. NATO had already established itself as the most successful and longest-lasting military alliance in modern history. Putin’s invasion has only served to strengthen NATO by rallying an unprecedented post-Cold War consensus within the alliance in favor of military preparedness and a shared commitment to deter aggression against any member. In addition, NATO member states have strongly supported the economic sanctions and other political measures to isolate Russia and raise the costs attendant to Russia’s continued fighting in Ukraine. Additionally, in May, political leaders in Finland and Sweden announced their intention to apply for NATO membership. The likely addition of two formerly neutral states to the alliance will further add to Russia’s discomfiture and NATO’s optimism about its ability to deter further aggression in Europe.

In the aftermath of Putin’s invasion and NATO’s likely expansion, however, complacency among member states should be avoided. Deterring Russia in the short term understates the demands that the international system and European politics will impose on an expanded NATO in the years to come. NATO’s political cohesion, military readiness, and escalation management skills will be essential for dealing with a variety of challenges and open questions. Among these include what to do with a post-Putin Russia; deterring and defeating transnational terrorism; the alliance’s relationship with a rising China; member states’ ability to maintain stable democratic regimes within their own countries and promote democratic institutions among non-NATO states; and adapting the alliance’s military strategy to a new world of technology that privileges cognitive warfare, space, and cyber capabilities.

The first issue is the political relationship between NATO and Russia after Putin either retires or is removed from office. For much of the 1990s, there was considerable optimism that post-Soviet Russia would be a more dependable strategic partner for NATO. Some even anticipated that a more democratic Russia might evolve from the ruins of the former Soviet Union. The whiff of optimism was soon dissipated, however, by events during the end of the 1990s, especially after NATO’s air war against Serbia over Kosovo. When former Russian president Boris Yeltsin resigned and turned over the presidency to Putin, the stage was set for a return to a more traditional Russian view of geopolitics with respect to the United States and NATO. Putin’s support for the U.S. invasion of Afghanistan in 2001 expedited cordial relations between the Russian president and U.S. president George W. Bush. But, by the time Bush departed from office, Putin had adopted a harder line toward NATO. Russia’s war with Georgia in 2008 marked a turning point that, with the advantage of hindsight, was a foretaste of things to come during the next fourteen years.

If Russia’s war against Ukraine is eventually settled by diplomatic negotiations following a protracted military conflict, then a postwar regime in Russia—with or without Putin—will have several options. First, it could maintain the revisionist stance toward the present rules-based international order in Europe and elsewhere. Second, it could adopt a more status quo-oriented policy that settles for a modus vivendi with an expanded NATO, pocketing small gains obtained in the war against Ukraine and, at least for the short term, gives up on the ambition of regime change in other European countries. Or it may move toward a détente with NATO and a more expansive policy of diplomatic, military, and cultural engagement with leading NATO powers, including the United States. The departure of Putin from office may push the lever toward the latter two options, although that depends upon the power struggle that follows him and the character of his successor.

A second issue for NATO will be its collective security agenda with respect to international terrorism. NATO support for U.S. military operations in Afghanistan was an essential component of U.S. combat and non-combat responses to the challenges posed by the Taliban and other non-state actors in that country. U.S. intelligence collaboration with NATO allies and within the Five Eyes group—consisting of the United States, United Kingdom, Australia, Canada, and New Zealand—is supported by global deployments of American special operations forces and other military and intelligence assets, including those of NATO allies. A robust network of information sharing tracks the military activities and communications of Al Qaeda and other major transnational terror networks. Although Biden’s national security strategy acknowledges that the United States now faces the problem of emerging peer competitors and the renewed threat of great power war, the threats posed by domestic and international terrorists have not gone away. In the wake of the U.S. military withdrawal from Afghanistan in August 2021, the Taliban, ISIS-K, and other groups with anti-American or anti-Western agendas will find new sanctuaries and outside support. These and other terrorist groups can use modern net-centric warfare to radicalize individuals across the globe and direct them against U.S. or allied targets. The possibility of a terrorist attack that uses weapons of mass destruction should also not be discounted as a continuing aspiration among radicals.

A third issue for NATO will be how to rethink its relationship with a rising China. China’s growing military and economic power challenges the Eurocentric international rules-based order and creates several security dilemmas for the United States and its allies. In addition to the immediate threat posed to Taiwan, China also creates military and political risks for Japan, South Korea, Australia, the Philippines, Vietnam, and other states in Asia. China’s long-range nuclear arsenal is growing—by the end of this decade, it is expected to deploy a triad of strategic nuclear launchers on land-based ballistic missiles, submarine-launched ballistic missiles, and long-range bombers. China’s sophisticated space program includes the ability to deploy satellites capable of shadowing other satellites or, if necessary, destroying them. Chinese cyberattacks against the United States and other countries regularly succeed in stealing intellectual property and classified government information. China’s Belt and Road Initiative, driven by a policy of buying up critical infrastructure for trade, manufacturing, and shipping, has increased its leverage over other governments and turned a much-ballyhooed form of globalization into a Chinese strategic triumph over whipsawed competitors. China’s continuing support for Russia will also capture NATO’s attention as Russia’s war in Ukraine continues to roil Europe.

A fourth issue that NATO must face is the fragility of democratic politics in a complicated twenty-first-century tapestry of ideologies and communications technologies. The twentieth century is a reminder that democracies can be toppled from within by adverse economic, political, and social forces. Timothy Snyder’s exemplary research has shown the potency of authoritarian appeals to a faux sense of nationalism and a reconstructed history, including in Russia. Europe as a collection of democratic countries based on consensual governments and pluralistic policymaking processes cannot be taken for granted. In the twenty-first century, a democratic Europe will face several challenges, including the growth of nationalist parties with anti-democratic agendas; changes in Western political cultures that privilege extremism and tribalism; the adverse consequences of “globalization,” including breakdowns in supply chains, the spread of pandemics, the disruption of markets, and the growth of an elite transnational class; and political coercion and military pressure from authoritarian regimes against democratic ones, within and outside of Europe.

Fifth, NATO will have to adapt its strategies and policies to emerging technologies for deterrence or warfighting in the space and cyber domains, human-machine interface, drone warfare, and unforeseen developments in bioengineering, nanotechnology, and cognitive science. If the twentieth century was the apogee of mass destruction in the industrial age, the twenty-first century will offer a variety of unconventional conflict settings, often combined with kinetic action. Major powers will be defined not only by the size of their military forces but also by how nimble and adaptive those forces are. Ukraine’s ability to defeat or slow the advances of Russian forces has illustrated the priority of adaptive learning and the superior use of intelligence, surveillance, and reconnaissance to support kinetic operations. Even future ground wars, notwithstanding those at sea or in space, will move at light speed. Commanders may be overwhelmed by mountains of data challenging their ability to separate the wheat from the chaff. The smart systems designed to unravel the chaos of battle will also contribute their own uncertainties to it.

How member states deal with these challenges will determine whether NATO continues to be the most successful military alliance in modern history. This is not the time for the alliance to lapse into complacency.

### 1AR — NATO Emerging Tech Key

#### NATO’s EDT innovation is vital to solve hybrid threats, deterrence, alliance cohesion, and strategic competition with Russia and China.

Magula and Alvarez-Couceiro 21 — Justin Magula, Army Strategist in the Strategic Landpower and Futures Group at the U.S. Army War College, holds an M.A. in International Public Policy from Johns Hopkins University, and Paula Alvarez-Couceiro, Analyst at Martin+Crumpton Group LLC—a global strategic advisory company based in Washington, DC, holds an M.A. in Strategic Studies and International Economics from Johns Hopkins University, 2021 (“Maintaining and Improving NATO’s Technological Edge,” *Wavell Room*, September 30th, Available Online at https://wavellroom.com/2021/09/30/maintaining-improving-natos-technological-edge-technology/, Accessed 07-04-2022)

What happens when an alliance’s competitors quickly improve their technology and capabilities to place the alliance at increased risk? The North Atlantic Treaty Organization (NATO) addressed this dilemma during a recent summit in Brussels. At the summit, the North Atlantic Council built upon NATO’s 2030 strategic outline and presented targets for increased technological collaboration to counter growing threats from Russia, China, and non-state actors. While NATO’s scientific and technical superiority has historically allowed it to outpace competitors, its adversaries are quickly closing the gap.

NATO members still hold advantages in their development of new technologies. According to the Global Innovation Index, seven of the top ten most innovative countries globally are part of NATO, while the other three are key NATO partners. Even so, NATO can do more to harness the alliance’s combined technological prowess to better compete and win in a future conflict. As China seeks to become the world’s innovation leader and Russia continues to undermine the alliance’s security, NATO will need to out-innovate its competitors and prepare for an uncertain future.

Four areas where NATO can focus on improving its competitive edge are developing its formal organizations, increasing public and private sector collaboration, harnessing and countering Emerging Disruptive Technologies (EDTs), and improving conventional military equipment. NATO must maintain its relative lead in technology sectors to defend its people and enhance its long-term strategic position. Improving science and technology (S&T) innovation will increase alliance collaboration, strengthen public and private sector cooperation, counter hybrid threats, deter adversaries, and harden defenses against attacks. NATO’s effectiveness in the future will heavily depend on its ability to maintain and improve its science and technology capabilities.

A Changing Environment

The global geopolitical situation has changed significantly over the past decade. Although NATO remains the world’s most successful and powerful alliance, China and other adversaries are quickly reducing NATO’s military and scientific advantages. In just the past year, China raised its defense budget by 6.8 percent and continues to build global power projection capabilities in addition to its regional defenses. As part of what some call a Fourth Industrial Revolution, Beijing is rapidly investing in AI, biotechnology, robotics, and other new technologies.

Russia is also developing new technologies, especially in areas where it can exploit NATO’s weaknesses. Russia’s ballistic missiles can reach anywhere in Europe, and Russia has placed renewed emphasis on improved missile technology, such as recent hypersonic advances. Russia has built a robust Anti-Access Area Denial (A2AD) network on Europe’s eastern flank while simultaneously expanding military capabilities into its Arctic region. Both areas pose direct security challenges to NATO, which the alliance’s S&T efforts can help mitigate.

Over the past decade, NATO has recognized the need for increased innovation and technological advancements. In 2012, the alliance created the Science and Technology Organization, taking on the former roles of the NATO Research and Technology Organization, including its executive function. It also incorporated the former NATO Undersea Research Center, established the NATO Chief Scientist position, and outlined the unified governance of NATO S&T. In 2020, NATO created an Innovation Board and an Advisory Group on Emerging and Disruptive Technologies to provide external advice to NATO on optimizing its innovation efforts.

At the 2021 Brussels Summit, NATO agreed to launch a civil-military Defense Innovation Accelerator for the North Atlantic (DIANA) to “foster transatlantic cooperation on critical technologies, promote interoperability and harness civilian innovation by engaging with academia and the private sector, including start-ups.” There are plans to establish a NATO Innovation Fund (NIF), where allies “can support start-ups working on dual-use emerging and disruptive technologies in areas key to Allied security.” These are steps in the right direction, but NATO can do more.

Expanding Technological Organizations

In conjunction with its newest additions, the DIANA and NIF, NATO can expand the capacities of its Science and Technology Organization (STO) to boost research and development (R&D) in artificial intelligence (AI), missile and missile defense technology, space, cyber, and other EDTs. The STO is the world’s largest defense and security research forum, employing over 6,000 scientists from allied nations. However, the STO does not turn NATO defense spending into tangible products or equipment for the alliance.

NATO could use the STO to streamline research and product development, ensuring all allies are working toward a common goal and not spending resources on identical R&D. For instance, each country could allocate part of its defense budget to develop standardized systems like integrated air, missile, and cyber defenses. Whether using the STO or DIANA as its main innovation driver, NATO must continue developing its formal institutions to harness solutions that benefit the entire alliance and help it achieve its three core tasks of collective defense, crisis management, and cooperative security.

Public and Private Sector Collaboration

The Brussels Summit Communique also recommends continuing the R&D of AI technologies and identifying alliance gaps in this critical focus area. Many of these advancements occur in the private sector, and NATO must find ways to use those technologies for the alliance. The U.S. National Security Commission on Artificial Intelligence’s March 2021 report states that AI-enabled warfare is part of the near future. While the United States and NATO are currently ahead in these technologies, other countries will soon pass them unless they increase their R&D efforts.

In addition to boosting research through the STO and DIANA, NATO can streamline the acquisition of commercial sector AI-focused technologies for national security purposes and create an alliance-wide process that acquires emerging technologies from the private sector. The rapidly changing nature of emerging technologies and the quantity and depth of innovation seen in the private sector require an acquisitions system that is not only fast but allows for the rapid integration of updated product iterations and innovations. Autocratic competitors excel in private and public sector integration, given the nature of their systems. Improving its ability to apply privately developed technology for military uses rapidly will ensure that NATO retains its competitive edge over its predominantly autocratic adversaries.

Harnessing and Countering Emerging Disruptive Technologies

While emerging and disruptive technologies (EDTs) touch all aspects of life and present exciting opportunities for the alliance, they also present threats. Many of NATO’s adversaries use EDTs against alliance personnel and infrastructure, such as recent cyberattacks targeting Polish politicians and the Colonial Pipeline. Enhancing its innovation processes will allow NATO to improve its military technology across all domains and boost its deterrence and defense capabilities. NATO could then better deter Russian and Chinese hybrid threats in cyber, space, electronic warfare, and information domains. For instance, NATO can use its forthcoming Cyber Command to take collective action and demonstrate cyberspace thresholds that will result in unified offensive cyber or conventional responses if crossed by its adversaries. By strengthening its cyber abilities and adding new capabilities, NATO can deter adversaries in the information space and take the offensive against them. NATO would then rob Russia and China of success in areas where they currently excel, and better protect the alliance’s people and infrastructure.

Conventional Military Improvements

NATO can also use its technological advancements to improve its conventional military capabilities. One critical area where NATO must focus is its integrated air and missile defense. Russian nuclear weapons can reach anywhere in Europe and NATO cannot adequately defend against new technologies like swarm warfare or hypersonic missiles. Two of NATO’s high-visibility modernization programs focus on combating air and missile threats, but NATO must do more to combat emerging and future adversary weapons.

As the United States continues R&D on a Patriot missile system replacement, NATO countries could ingrate into its supply chain, like that of the F-35 aircraft, or develop complementary systems that fill gaps in the U.S. air defense system’s effectiveness. The current NATO Integrated Air and Missile Defense system uses mainly American-made radars and missiles stationed in NATO countries. While effective, NATO could harden its defenses by fielding European-developed systems that are compatible with current and future U.S. systems, thus expanding its anti-access area denial (A2/AD) bubble while simultaneously reducing air and missile threats. Furthermore, the alliance can conduct more combined military exercises to test new equipment and boost unit proficiency. Improving its deterrence and defenses in critical areas will reduce the military threats from NATO’s adversaries as they seek to sow division and destabilize the alliance. When it couples military advances with other areas of technological improvement, NATO gains the best chance of maintaining its competitive edge.

NATO will still need to overcome bureaucratic hurdles across its 30-member alliance. As Nicholas Nelson of the Center for European Policy Analysis (CEPA) notes, for the DIANA and NIF “to succeed, they must address authority and budget concerns, and then bring in the right personnel to lead and staff them.” Even so, NATO is taking the proper steps to improve its scientific and technological capabilities. Its strategic documents reflect the importance it is placing in these areas. By creating new institutions, NATO is setting the foundation for further development and expanded capabilities.

Given the threats that adversaries pose to the alliance, maintaining and improving its scientific and technological prowess will be vital to NATO’s future success. Strengthening these areas will boost military effectiveness, deterrence, and defense and enhance private and public cooperative advancements. It will ultimately give the alliance more strategic flexibility while improving NATO’s defenses in areas beyond the military, such as energy and cybersecurity in the private sector. By continuing to out-innovate its competitors, NATO will protect its people and infrastructure, and ensure that the alliance remains prepared to combat any challenges from Russia or China.

#### Integrated NATO-wide EDT innovation is key to interoperability and alliance cohesion.

Soare 21 — Simona R. Soare, Senior Associate Analyst at the European Union Institute for Security Studies, former Security and Defence advisor to the Vice President of the European Parliament, former Defence Analyst with the Ministry of Defense of Romania, holds a Ph.D. in Political Science from the National School for Political and Administrative Studies (Romania), 2021 (“Innovation as Adaptation: NATO and Emerging Technologies,” German Marshall Fund of the United States Policy Brief, June, Available Online at https://www.gmfus.org/sites/default/files/Soare%2520-%2520NATO%2520emerging%2520tech.pdf , Accessed 07-18-2022, p. 8)

Pursuing Collaborative Innovation

Not all allies have the defense funding, technological capacity, skills, and military infrastructure to facilitate rapid defense innovation, including the adoption and scaling of emerging technologies. And not all that have such resources and knowledge are willing to share them in collaborative innovation processes. Leading allies—the United States, France, the United Kingdom, and the Netherlands—already have national-focused approaches to the adoption of EDTs. By contrast, for most Central and Eastern countries EDTs in defense are mainly a long-term prospect. Previous challenges in integrating cyber capabilities into NATO operations, persistent capability gaps among the allies, and slow standardization procedures are a good indication of the magnitude of the challenge, which is acknowledged at the highest levels of NATO decision-making.

As Secretary-General Stoltenberg has stated, a technological gap between the allies would undermine interoperability and weaken alliance cohesion. In the context of the NATO AI and big data strategies and the Defense Innovation Accelerator, allies should reflect on how to improve and facilitate technological transfers among themselves. This could enable smaller allies to specialize in niche EDTs capabilities, as has been the case with cyber, for example, and could prevent the emergence of new technological and capability gaps between the allies. The Biden administration’s focus on shared democratic values and the digital agenda, and its willingness to strengthen NATO and technology partnerships, constitute a window of opportunity for the alliance. It should be fully capitalized on to accelerate transatlantic collaborative defense innovation.

#### NATO’s EDT innovation is key to beat Russia and China.

Becker et al. 22 — Jordan Becker, Assistant Professor of International Relations and Director of the Social Sciences Research Lab at the United States Military Academy (West Point), Lieutenant Colonel in the U.S. Army, holds a Ph.D. in War Studies from King’s College London (UK), et al., with Douglas Lute, Chair of International and Defense Practices at BGR Group—a lobbying firm, former U.S. Permanent Representative to NATO (from 2013 to 2017), former Deputy National Security Advisor for Iraq and Afghanistan on the White House National Security Council (from 2007 to 2013), former Lieutenant General in the U.S. Army where he served as Director of Operations at U.S. Central Command, holds an M.P.A. from Harvard University, and Simon Smith, Associate Professor in the School of Justice, Security, and Sustainability at Staffordshire University (UK), former Research Officer in the Department of Politics, Languages, and International Studies at the University of Bath (UK), former University Teacher and Administrator for the Centre for the Study of International Governance at Loughborough University (UK), holds a Ph.D. in International Relations from Loughborough University, 2022 (“Don’t Let Russia Dominate the Strategic Concept,” *War on the Rocks*, June 28th, Available Online at https://warontherocks.com/2022/06/dont-let-russia-dominate-the-strategic-concept/, Accessed 07-12-2022)

New Domains

Whether in coordination or not, China and Russia will undoubtedly continue to challenge allies in domains like space and cyber using emerging and emerged technologies. Dealing with such challenges is core NATO business — grounded in Article 3 of the Washington Treaty and resting primarily with national authorities. The new Strategic Concept should aim to integrate these relatively new domains while responding to disruptive technologies as well. Allies must endeavor to reach a “pre-crisis” consensus on what space and cyber actions would constitute an “armed attack” in accordance with Article 5. This kind of crisis decision-making is a core function of NATO’s political and military headquarters. Such agreement, when paired with improved national capabilities, would contribute to deterrence by communicating resolve to adversaries. Improved capabilities themselves will only arise through public-private partnership to maintain a technological edge. A common strategic culture of innovation, much of which arises from the private sector, is a key advantage that NATO has — and should retain — over its adversaries. Such innovation has been on display in the Russo-Ukrainian war and will doubtless be essential in future conflicts.

### 2AC — U.S. Key To Ally Follow-On

#### U.S. Key To Ally Follow-On — it determines their support.

Binnendijk and Priebe 19 — Anika Binnendijk, Political Scientist at the RAND Corporation, former Staff Member in the Office of Policy Planning and the U.S. Department of State, former Special Assistant and Policy Advisor in the Office of the Secretary of Defense for Policy at the U.S. Department of Defense, holds a Ph.D. in International Relations and National Security Studies from The Fletcher School at Tufts University, and Miranda Priebe, Political Scientist at the RAND Corporation, holds a Ph.D. in Political Science from the Massachusetts Institute of Technology, 2019 (“Factors Affecting an Ally’s Decision to Provide Military Support,” *An Attack Against Them All? Drivers of Decisions to Contribute to NATO Collective Defense*, Published by the RAND Corporation, ISBN 9781977402776, Available Online at https://www.rand.org/content/dam/rand/pubs/research\_reports/RR2900/RR2964/RAND\_RR2964.pdf, Accessed 07-15-2022, p. 20-22)

Participation of Other Allies

As an ally weighs a potential contribution to collective defense, it is likely to consider who else is participating.63 Research on alliance burden-sharing has focused on a mix [end page 20] [Table Omitted — see URL] of rational calculations and the normative considerations that states make. Some analysts have applied collective action theory to explain why, during peacetime, smaller NATO allies are likely to minimize contributions or freeride. If these allies believe that others will provide collective defense—even if they do not contribute—they have little to gain by burden-sharing. However, this dynamic would be less applicable in the event of a conventional Russian attack for two reasons. First, as detailed below, states that do not contribute could be punished more harshly by other allies for failing to respond to a Russian attack than they are in peacetime. Second, each ally’s contributions could materially affect the outcome if the crisis were to escalate to a wider war.64 Put another way, in the face of an overwhelming common security threat—direct conflict with Russia—a freeriding approach could potentially be more costly for NATO members than burden-sharing.65 [end page 21]

Allies will also consider whether the operation has enough military support to be successful. Whether the United States—the strongest member of the alliance—contributes could be critical to the coalition’s prospects for success. If the United States is making significant contributions, an allied government might feel more confident in the operation and, therefore, be more willing to contribute.

### 1AR — U.S. Key To Ally Follow-On

#### Integrated transatlantic EDT innovation is key to solve the case and NATO cohesion — the plan’s key to remove the U.S.’s signal of distrust.

Fiott 21 — Daniel Fiott, Security and Defense Editor at the European Union Institute of Security Studies (France), Visiting Professor at the The Institute for European Studies at the Vrije Universiteit Brussel (Belgium), holds a Ph.D. in Political Science from Vrije Universiteit Brussel (Belgium), 2021 (“Promoting Technological Sovereignty and Innovation: Emerging and Disruptive Technologies,” German Council in Foreign Relations Workshop Report Number 21, Edited by Christian Mölling and Florence Schimmel, November, Available Online at https://www.ssoar.info/ssoar/bitstream/handle/document/75843/ssoar-2021-molling\_et\_al-Promoting\_Technological\_Sovereignty\_and\_Innovation.pdf, Accessed 07-17-2022, p. 7-8)

3.9. How to enhance EU-NATO complementarity on EDTs?

The NATO alliance increasingly sees itself as a “transatlantic forum” on EDTs. This aim has been stressed during the NATO 2030 reflection process. NATO fears that EDTs are proliferating into the hands of adversaries, and this is eroding the alliance’s military-technological superiority. NATO also recognizes that the growth of EDTs poses a risk with regard to alliance cohesion because unequal development and ownership of EDTs can lead to lower interoperability and higher technology gaps. While the alliance has a proven track record of developing standards, NATO has neither the financial resources nor regulatory power to take a comprehensive lead on the question of EDTs. This situation has even given rise to new ideas such as a NATO Innovation Fund and the Defense Innovation Accelerator for the North Atlantic (DIANA).2 There is certainly scope for more EU-NATO [end page 7] common engagement with the strategic challenges and opportunities that could emerge due to EDTs. In fact, the EU’s Political and Security Committee and the North Atlantic Council met in March 2021 to discuss EDTs.

3.10. Technological sovereignty in a transatlantic context

The development of EDTs touches on the sensitive issue of industrial competitiveness. Technological sovereignty implies mastery and control of technology. This is certainly the case in the United States, where two early Executive Orders under the Biden administration target domestic technological competitiveness (“Buy America”) and global critical supply chains. There is a fear that promoting EDT uptake within NATO is a way to enhance the competitiveness of American firms that develop EDTs; the US already has a comparative advantage in many critical technology sectors. A key question for the EU then, is how to engage in a transatlantic dialogue on EDTs without harming its own industrial competitiveness or control over critical technology sectors. Proposals such as the EU-US Trade and Technology Council or the EU-US Defense Dialogue could help to work out differences over regulations, standards, extra-territorial measures, forced transfers of technology, and intellectual property rights. 3

### 2AC — Alliance Fragmentation Deficit

#### Alliance Fragmentation Deficit — integrating Euro-Pacific alliances is essential for effective deterrence and maintaining U.S. power.

Simón 22 — Luis Simón, Argyros Family Foundation Visiting Fellow with the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies, Director of the Brussels Office of the Elcano Royal Institute (Spain), Research Professor in International Security and Director of the Centre for Security, Diplomacy, and Strategy at the Brussels School of Governance (Belgium), holds a Ph.D. in International Relations from the University of London (UK), 2022 (“Bridging U.S.-Led Alliances in the Euro-Atlantic and Indo-Pacific: An Inter-theater Perspective,” Center for Strategic and International Studies, May 12th, Available Online at https://www.csis.org/analysis/bridging-us-led-alliances-euro-atlantic-and-indo-pacific-inter-theater-perspective, Accessed 07-15-2022)

The Issue

Although U.S. strategic competition with China and Russia is often presented as a challenge with two separate fronts, this brief argues that the Euro-Atlantic and Indo-Pacific theaters are increasingly linked. Insofar as preserving a favorable balance of power in these two regions hinges largely on U.S. power, and as long as they both continue to exercise a significant pressure on U.S. defense resources, their alliance and deterrence architectures should be looked at from an inter-theater perspective. Thus, optimally managing a two-front challenge would require a serious effort to bridge U.S.-led alliances in both regions.

Introduction

The war in Ukraine, and the need to deter further Russian aggression in Eastern Europe, has triggered a debate about the United States’ ability to adequately resource a much-needed rebalance to Asia and prioritize strategic competition with China. For some, Ukraine is a dangerous distraction: the United States should avoid getting bogged down in Europe, lest it incentivize Beijing to engage in opportunistic aggression in Asia.1 According to this line of thinking, deterrence in Asia, and the security of the United States’ Indo-Pacific allies, hinges on U.S. restraint in Ukraine and in Europe more broadly.2 Others, however, argue that a hot war and the prospect of further military aggression will inevitably compel the United States to strengthen its posture in Europe in the foreseeable future.3 This does not mean that Washington should take its eyes off China. Rather, it should prepare to deter and win a war on two fronts simultaneously.4 A Russian failure in Ukraine could conceivably change U.S. calculations over the medium term and even lay the groundwork for a proper strategic rebalance to Asia.

Should the United States establish a clear priority between Russia and China or go all in on both fronts? What are the implications of each option for U.S. defense strategy? And where do the United States’ European and Asian allies come into the picture? U.S.-allied dominance at sea and the preservation of favorable balances of power in Europe and East Asia should be seen as interdependent concepts or parts of a “geostrategic trinity” of power, upon which the open, rules-based international system largely rests. As long as preserving a balance of power in Europe and East Asia hinges largely on U.S. power, and as long as these two regions continue to exercise a significant pressure on U.S. defense resources, their alliance and deterrence architectures will probably remain intertwined. The question is not so much which region matters most or under which circumstances. The unraveling of the balance of power in one region would punch a hole in the U.S.-led forward defense perimeter in Eurasia, endanger U.S.-allied dominance at sea, and eventually threaten the balance in the other region. Hence the United States’ European and Asian allies have a stake in the preservation of favorable balances of power in each other’s region and in U.S. maritime dominance more broadly. It is also why the U.S.-led deterrence and alliance architectures in Europe and Asia should be looked at from an inter-theater perspective.

Russia’s invasion of Ukraine has prompted the mobilization of countries such as Japan, Australia, and South Korea, who have joined the sanctions imposed by the United States and the European Union and provided their own support to Ukraine. Building on such political momentum would allow to promote an inter-theater approach to deterrence and alliances in Europe and East Asia. Critically, such an inter-regional approach can allow the United States and its allies to collectively navigate the two-front problem and adequately resource deterrence in Europe and East Asia simultaneously. Even though mutual defense commitments may remain intra-regional, as opposed to inter-regional, greater coordination between U.S.-led alliances in the Euro-Atlantic and Indo-Pacific could help ensure an optimal allocation of U.S. and allied strategic resources. Specifically, both sets of alliances should upgrade consultation mechanisms at the political and military levels and apply an inter-theater lens to burden sharing, force planning, and posture.

### 1AR — Alliance Fragmentation Deficit

#### Integrating innovation networks is key to create economies of scale and cement allied superiority.

Simón 22 — Luis Simón, Argyros Family Foundation Visiting Fellow with the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies, Director of the Brussels Office of the Elcano Royal Institute (Spain), Research Professor in International Security and Director of the Centre for Security, Diplomacy, and Strategy at the Brussels School of Governance (Belgium), holds a Ph.D. in International Relations from the University of London (UK), 2022 (“Bridging U.S.-Led Alliances in the Euro-Atlantic and Indo-Pacific: An Inter-theater Perspective,” Center for Strategic and International Studies, May 12th, Available Online at https://www.csis.org/analysis/bridging-us-led-alliances-euro-atlantic-and-indo-pacific-inter-theater-perspective, Accessed 07-15-2022)

An inter-theater approach to capability development can help preserve the dominance of U.S.-led alliances in both theaters. Even though some U.S. capabilities are global, others will be theater-specific and require adaptations. For instance, “theater-range” missiles may need to adapt to specific range or platform requirements (i.e., sea-borne vs. land-borne) depending on whether they are intended for Europe or Asia. This applies to both offensive and defensive missiles. Including allies in U.S.-led capability planning initiatives can generate economies of scale and make it easier for the United States to develop skeleton concepts that can draw on allied support and participation to bring about appropriate adaptations for each theater. Moreover, the need to preserve dominance at sea and in other global commons should also incentivize inter-allied cooperation in developing naval, air, cyber, and space capabilities and technologies.

Strengthening links between U.S.-led alliances in the Euro-Atlantic and Indo-Pacific in the area of operational planning would give both sets of allies greater insight into the military-strategic picture in each other’s region and how such a picture may affect U.S. and allied planning in real time. It would also allow them to assess possible implications for their home region and identify opportunities to add value in each other’s region, as well as in underpinning U.S. and allied dominance at sea and in the other global commons. Thus, allies could consider the establishment of permanent liaison officers from AP4 countries in Supreme Allied Command Europe and throughout NATO’s command structure, as well as a NATO liaison cell in U.S. Indo-Pacific Command, and more joint exercises.42

Ultimately, an effort to bridge U.S.-led alliances in the Euro-Atlantic and Indo-Pacific would help transcend the China first vs. two-front war dilemma and allow the United States and its allies to develop an optimal collective strategy to underpin the geostrategic trinity of their power. This becomes particularly relevant when the United States and its allies face two strategic competitors in two distant regions simultaneously and in light of Sino-Russian strategic cooperation. Should one of those competitors collapse, or should there be a breakdown in Sino-Russian ties, the need for alliance bridging may indeed become less evident or urgent. Hence, policymakers should pursue flexible and pragmatic approaches to bridging allies that eschew creating new institutions and respect the primacy of regional frameworks, which are arguably more lasting.

## AT: Germany-Italy CP

### 2AC — No Strategic Autonomy Net-Benefit

#### No Strategic Autonomy Net-Benefit — it’s impossible and counter-productive.

Davidson 22 — Jason W. Davidson, Professor of Political Science and International Affairs at the University of Mary Washington, Nonresident Senior Fellow in the New American Engagement Initiative at The Atlantic Council, holds a Ph.D. in Government from Georgetown University, 2022 (“European Strategic Autonomy Is Dead,” *The National Interest*, June 28th, Available Online at https://nationalinterest.org/feature/european-strategic-autonomy-dead-203222, Accessed 07-15-2022)

On the eve of NATO’s Madrid Summit, one fact of European security has become increasingly clear: NATO is the only feasible guarantor of the security of European states and, thus, the European Union’s (EU) objective of achieving strategic autonomy is unlikely to become a reality anytime soon.

In the early days following Russia’s invasion of Ukraine, it would have been reasonable to expect the war would provide the necessary impetus for the European Union to finally achieve strategic autonomy. Unity develops in response to a common threat and Russia’s attack demonstrated its aggressive intentions. Moreover, the Russian threat was such a shock that it seemed to cause a “sea change” in defense policy for many European governments. The Biden administration had already rightfully signaled that it would welcome greater European responsibility for defense and security, as it would allow the United States to focus more on the greater threat posed by China. In a further positive development, the EU published a “Strategic Compass,” outlining its plans for improved defense and security cooperation, only a month after the Russo-Ukrainian War began.

In the months since, however, it has become clear that European strategic autonomy is unlikely to come to fruition anytime soon: the war has increased the stakes and made apparent the risk involved in forming an alternative to NATO, major EU members France and Germany have acted in ways that cast doubt on their ability to lead, and Sweden and Finland’s NATO application demonstrates that the backing of the United States is the only real guarantee against Russian aggression.

While European autonomy in defense and security has long been a goal, President Donald Trump’s criticism of NATO and expressed desire to withdraw from the alliance, led many European policymakers to search for alternatives to the Atlantic alliance. What do advocates of strategic autonomy mean by the term? In a November 2019 interview with The Economist Emmanuel Macron declared NATO’s “brain death” and said “Europe must become autonomous in terms of military strategy and capability,” later claiming that “Europe has the capacity to defend itself.” Within a week of Russia’s invasion of Ukraine, Macron proclaimed that “Europe must invest more in order to decrease its dependence on other continents and to be able to decide for itself. In other words, it must become a power that is both more independent and more sovereign.” So, strategic autonomy, in the view of its leading proponent, would mean an EU that is capable of defending its members without assistance from the United States.

Russia’s attack on February 24, 2022, demonstrated aggressive intentions fundamentally greater than anything it has done since the end of the Cold War. Russia’s full-scale invasion of Ukraine suggested to Europeans that a Russian attack on an EU or NATO member, while not likely, is no longer unthinkable. Given this new reality, the stakes of choosing the right security architecture are higher than they have been for decades. If European countries bet on an unknown and untested EU for their defense, they would risk attack, territorial loss, and even subjugation. Finally, while the early weeks of the war demonstrated Russian military incompetence, experts warn that Russia has learned from mistakes, retains destructive military capabilities, and will likely use its oil and gas sales to rebuild its war machine.

France and Germany—the EU’s top two economies, largest military spenders, and loudest advocates for strategic autonomy—have acted in ways that have made strategic autonomy less likely. First, many European leaders—especially those bordering Russia—view French and German calls for Ukraine to make compromises with Russia with great concern. From the perspective of those countries most concerned with the Russian threat, the appeal to a diplomatic solution could mean they are forced to give up territory for the sake of the greater good. When asked recently about German mediation attempts, an Eastern European diplomat said “[w]e don’t need German protection; history proved it to be on the wrong side of history.” Second, there is a well-documented gap between the military capacity of EU member states and what they would need to be truly autonomous in defense. Despite initial indications to the contrary, it now seems increasingly unlikely that Germany will engage in a significant change in its defense spending and strategic culture, which will thwart the move towards European strategic autonomy. Aside from the contribution Germany—as the EU’s wealthiest member—will not make toward enhanced European defense capacity, its inaction will signal to other Europeans that are still not bothered by the Russian threat that it is fine to return to the pre-war levels of defense spending. Finally, there is the issue of France’s nuclear arsenal. The United States has extended its nuclear deterrent to cover NATO members, whereas France’s nuclear arsenal defends its territory and vital interests, not the EU or NATO.

The recent decision by the governments of Sweden and Finland to apply for NATO membership is the death knell for EU strategic autonomy. Both countries are EU members, so both should—in theory—be protected by the Lisbon Treaty’s Article 42 defense clause. Moreover, both countries understand that the act of applying to NATO would draw Russia’s ire and potential coercive measures to keep them out of the alliance and impose costs on them. They also knew that there would be at least a few months between when they applied for membership and when they received the full protection of NATO’s Article V mutual defense clause (Turkey’s objections have extended that timeline). As such, if they believed that EU strategic autonomy could provide them with sufficient protection from Russia in the near to medium term, it would have been rational to continue to remain outside of NATO. But Sweden and Finland have chosen otherwise. A May 2022 Swedish Foreign Affairs report stated: “It is clear that there is a lack of political will among EU Member States to develop collective defence within the EU.” While NATO certainly faces challenges, Sweden and Finland’s applications suggest the alliance provides a better security blanket against a Russian attack than the EU.

What if Donald Trump or a Trump-aligned, NATO-critical Republican wins the 2024 U.S. presidential election? Wouldn’t that outcome force Europeans to return to strategic autonomy? First, given the American public’s bipartisan concern with the threat posed by Russia since its attack on Ukraine, it would not be politically expedient for a Republican nominee to emphasize criticisms of NATO in the way that Trump did previously. Second, while Trump’s rhetorical criticisms of NATO were fierce, his administration’s policies toward the alliance were quite favorable. Finally, the Russo-Ukrainian War is likely to lead more NATO states to meet the 2 percent of gross domestic product defense spending goal, lessening one of Trump’s most salient criticisms of the alliance.

Given the death of EU strategic autonomy—and the United States’ continued interest in European security—NATO will remain the critical security mechanism for Europe. The United States will have to remain engaged in Europe, even as it focuses more on Asia, though it should be able to use the residual threat from Moscow to leverage greater European contributions to their own defense.

### 1AR — No Strategic Autonomy Net-Benefit

#### Strategic autonomy doesn’t make sense post-invasion.

Mason 22 — Paul Mason, British freelance journalist and commentator, former Visiting Professor of Economics University of Wolverhampton, former Economics Editor at Channel 4 News, former Business Editor at BBC’s *Newsnight*, 2022 (“Ukraine, NATO and a Zeitenwende,” *Social Europe*, April 11th, Available Online at https://socialeurope.eu/ukraine-nato-and-a-zeitenwende, Accessed 07-04-2022)

‘Strategic autonomy’

So the second big piece of reframing has to involve European ‘strategic autonomy’. Long pursued by Macron, this has been given impetus by the Zeitenwende (historical turn) declared by the German chancellor, Olaf Scholz.

Before Putin attacked Ukraine, one could argue that the EU needed strategic autonomy because the US was no longer a reliable ally, European capitalism needed to exert some sovereignty over technology and information, and the European powers needed to ‘take the strain’ from America in deterring Russian aggression. Europe would then find its own centre of gravity, in security terms, with Russia.

Strategic autonomy remains worthy of support but the Russian invasion—and the two draft treaties, with NATO and the US, which Putin slapped on the table in December—change things. It is vital, for the next ten years at least, to keep the US actively engaged in the defence of NATO’s eastern flank. That means NATO, not the EU, playing the leading role in Europe’s security. Idealism might make us wish this were otherwise; realism demands recognising the facts.

### 2AC — German Investment Fails

#### German Investment Fails — procurement bureaucracy and strict export controls prevent innovation and allied cooperation.

Schütz et al. 22 — Torben Schütz, Associate Fellow in the Security and Defence Program at the German Council on Foreign Relations, Research Fellow at the Defense AI Observatory and Ph.D. Candidate at Helmut Schmidt University/University of the Federal Armed Forces Hamburg (Germany), et al., with Joseph Verbovszky, Research Fellow at the Defense AI Observatory and Ph.D. Candidate at Helmut Schmidt University/University of the Federal Armed Forces Hamburg (Germany), holds an M.A. in International Relations and Economics from Johns Hopkins University, holds an M.A. in History and Political Science from Case Western Reserve University, and Heiko Borchert, Co-Director of the Defense AI Observatory at Helmut Schmidt University/University of the Federal Armed Forces Hamburg (Germany), Associate Fellow at the Center for Advanced Security, Strategic, and Integration Studies (Germany), Senior Research Fellow at the German Institute for Defence and Strategic Studies, holds a Ph.D. in International Relations from the University of St. Gallen (Switzerland), 2022 (“Beware of Potemkin: Germany’s Defense Rethink Risks Reinforcing Old Habits,” *War on the Rocks*, April 11th, Available Online at https://warontherocks.com/2022/04/beware-of-potemkin-germanys-defense-rethink-risks-reinforcing-old-habits/, Accessed 07-17-2022)

Executing: Walk the Talk

Finally, a true Zeitenwende would demonstrate a new focus on proper policy execution and disentanglement from the institutional inertia currently prevalent in the parliament, government, and bureaucracy. Right now, however, the odds are against readjusting the defense enterprise towards performance.

Currently, the lack of precise and actionable political guidance is hampering action to reform the most crucial stumbling block of efficient and effective armament procurement: the Bundeswehr’s procurement agency. Risk-averse bureaucrats, prolonged lawsuit-heavy procurement processes, indecision and incoherent signaling on the political level, massive delays in industrial delivery, excessive cost overruns, equipment without promised features, the low quality of delivered equipment, and the need for the defense industry to fully comply with criteria based on civilian safety requirements are the most common complaints. Hence, the current German procurement system, including industrial production capacities, looks ill-equipped to handle even more money without running the risk of wasting it. Additionally, its overall absorption capacity across all stages of the armament’s life-cycle — research and development, design, contractual negotiations, production, certification, operation and maintenance, and disbursement — is limited.

Furthermore, and true to its roots, Germany will likely retain its restrictive arms-export policy. During the special parliamentary session, Foreign Minister Annalena Baerbock not only used her speech to explain why Germany greenlighted the arms exports to Ukraine, but she also seized the opportunity to highlight the exceptionalism of this decision. Societal pressure will grow as increased domestic defense spending potentially alleviates export dependencies and economic pressures for Germany’s defense industry. Moreover, as more and more E.U. and NATO allies are announcing national spending increases, which traditionally generates strong demand for the German defense industry, economic incentives for exports beyond E.U., NATO, and NATO-equivalent countries further decrease. Activists critical of German arms exports have repeatedly urged Germany to focus on domestic and allied markets, as further illustrated, for example, by a recent study commissioned by Greenpeace. This is especially true as German society and politicians are most critical of exports beyond allied countries. However, as seen in past years, Germany’s strict export practice also negatively impacts multinational armaments projects, resulting in diplomatic grievances with even its closest allies. The combination of these factors doesn’t necessarily bode well for further defense industrial and armament cooperation envisaged, for example, as part of the European Defense Fund, aiming to promote collaborative multinational research and development, or NATO’s new Defense Accelerator for the North Atlantic, which focuses on intensifying transatlantic development in dual-use technologies.

Although important, spending more on defense is not enough. For Scholz’s Zeitenwende to deliver true change, Germany needs to spend differently and embed the spending hike in a broader national and international context.

### 2AC — Italian Investment Fails

#### Italian Investment Fails — it’s too fragmented and bureaucratic.

Marrone and Gilli 20 — Alessandro Marrone, Head of the Defence Programme at the Instituto Affari Internazionatli (Italy), Professor at the Istituto Superiore di Stato Maggiore Interforze of the Italian Ministry of Defence, holds a Ph.D. in History of Europe from La Sapienza University of Rome (Italy), and Andrea Gilli, Senior Researcher in Military Affairs at the NATO Defense College (Italy), Affiliate of the Center for International Security and Cooperation of Stanford University, holds a Ph.D. in Social and Political Science from the European University Institute (Italy), 2020 (“Defence Innovation: New Models and Procurement Implications: The Italian Case,” Armament Industry European Research Group Policy Paper #64, October, Available Online at https://www.iris-france.org/wp-content/uploads/2020/10/64-DefInnov-Italy.pdf, Accessed 07-17-2022, p. 3-4)

A Fragmented, Applied Research

The way the Italian defence establishment has managed technological innovation so far has a set of implications. First, the focus is on applied rather than basic research, usually involving an elevated Technology Readiness Level (TRL). Secondly, innovation is fragmented across procurement programmes, thus preventing both cross-fertilization and economies of scale. Thirdly, programmes are mainly attached to one service, as a result the joint level inevitably receives less attention and resources, to the detriment of critical areas such as missile defence and the whole cyber domain including the digitalisation of military equipment. Last but not least, the world of defence in Italy is relatively globally closed to Small and Medium Enterprises (SMEs), start-ups and mid-caps companies operating in the civilian sector. Overall, because of this complex system where not all incentives and priorities are aligned, a long-term, comprehensive strategy for defence innovation is very difficult to achieve and, eventually, to implement.

The R&T funds not linked to a specific procurement are managed through the Piano Nazionale di Ricerca Militare (PNRM). The PNRM is the Ministry of Defence’s national plan for military research: its budget is extremely limited, about € 50 million per year, and it covers a relatively high number of projects. [end page 3]

An additional factor complicates defence innovation in Italy: defence investments are split between the MoD and the Ministry of Economic Development, with the former allocating around € 2-2.5 billion per year to defence procurement involving Italian industries. Such a funding does include R&T activities, but its exact extent is unclear given that such activities are included in various forms within single procurement programmes. The two ministries have to cooperate both at the political and practical level to finance projects satisfying the needs of the armed forces, and this entails a set of bureaucratic hurdles.

## AT: Quadrilateral Security Dialogue CP

### 2AC — Quad Innovation Fails

#### Quad Innovation Fails — multiple barriers.

Goodman 21 — Matthew P. Goodman, Senior Vice President for Economics and Simon Chair in Political Economy at the Center for Strategic and International Studies, former Director for International Economics and Director for Asian Economic Affairs at the U.S. National Security Council, former Senior Adviser to the Undersecretary for Economic Affairs at the U.S. Department of State, former International Economist at the U.S. Treasury Department, holds an M.A. in International Relations from Johns Hopkins University, 2021 (“Allied Technology Cooperation: Opportunities and Challenges,” Center for Strategic and International Studies, March 23rd, Available Online at https://www.csis.org/analysis/allied-technology-cooperation-opportunities-and-challenges, Accessed 07-18-2022)

On March 12, U.S. president Biden, Japanese prime minister Suga, Indian prime minister Modi, and Australian prime minister Morrison attended the first leader-level summit of the Quadrilateral Security Dialogue, or Quad. The resulting joint statement pledged to deepen the nascent grouping, which arose in response to the 2004 Indian Ocean tsunami but lay dormant from 2008 to 2017, and to expand its focus beyond military exercises and humanitarian aid. Notably, the Quad leaders established three working groups to collaborate on Covid-19 vaccine distribution, climate action, and critical and emerging technologies. The technology working group is the latest of several recent efforts to formalize cooperation among like-minded countries on protecting, regulating, and developing strategic technologies. Since the election of President Biden, such proposals have gained steam, ranging from new multilateral bodies to narrowly scoped technical efforts. Yet there remain significant hurdles to the sort of broad technology partnerships envisioned.

Q1: What is the impetus for cooperation on critical technologies?

A1: The United States and its allies have a history of joint research and protection of critical technologies, dating back to British and Canadian support for the Manhattan Project. Today, China’s rapid technological advancement and ambitious industrial strategy have raised concerns in Washington and other allied capitals that Beijing will lead the deployment of emerging technologies, such as artificial intelligence and quantum computing, which could have problematic economic, strategic, and human rights implications.

U.S. policymakers worry that Chinese government-backed firms could undercut U.S. competitors, potentially pushing them out of business and eroding the defense innovation base. In addition, the ongoing semiconductor shortage and recurring fears that Beijing could limit access to strategic minerals have bolstered calls for secure, resilient supply chains. Finally, Washington and its allies have a shared interest in ensuring that the development of emerging technologies, as well as the evolving standards and regulations that govern them, align with democratic values.

Q2: What is being proposed?

A2: Given the international nature of global technology supply chains and talent, multilateral cooperation can more effectively address concerns posed by China. The Biden administration has made such coordination the cornerstone of its foreign policy agenda, and U.S. allies and partners have similarly emphasized the need to work together.

The Biden administration’s Interim National Security Strategic Guidance released in early March envisions joining with “like-minded democracies to develop and defend trusted critical supply chains and technology infrastructure,” as well as “promoting shared norms and forg[ing] new agreements on emerging technologies.” The U.S. Congress has taken initial steps to support such cooperation. The 2021 National Defense Authorization Act authorized two funds for joint development and production of telecommunications and microelectronics technologies, although these have yet to receive appropriations. Several pieces of pending legislation would support broader cooperation. For example, the bipartisan Democracy Technology Partnership Act would seek to align standard-setting, data governance, tech transfer policies, supply chain reorganization, and research and development (R&D) promotion among advanced democracies.

U.S. allies have made other proposals in the spirit of cooperation. In its December 2020 New EU-U.S. Agenda for Global Change, the European Commission proposed an EU-U.S. Trade and Technology Council to strengthen joint technological leadership. The United Kingdom’s March 2021 Integrated Review of Security, Defence, Development and Foreign Policy endeavors to “develop a new framework for international science partnerships” and put technology at the core of alliances. Japan maintains roughly 160 joint scientific research collaboration projects with the United States and has been supportive of expanding the Quad format to cover emerging technology.

Outside policy experts have also tabled various ideas, such as an informal “Technology 10” forum that would coordinate on global standards and supply chains with variable, issue-specific membership.

Q3: Where do the proposals diverge?

A3: While all under the aegis of allied technology cooperation, the proposals differ on scope. Most cover technology protection and standard-setting, but some also include joint development efforts and even competition policy harmonization.

Among official proposals, the European Commission’s Trade and Technology Council is the broadest. The plan encompasses “developing compatible standards and regulatory approaches for new technologies, ensuring critical supply chain security, deepening research collaboration, and promoting innovation and fair competition.” Notably, the document links trade and technology issues and emphasizes the imperative of “solving bilateral trade irritants that weaken our strategic partnership.” Unlike other frameworks, the European Commission’s proposes that competition policy—a complicated subject for Washington—be discussed in a “transatlantic dialogue on the responsibility of online platforms and Big Tech.”

The Biden administration has not yet put forward a detailed, public vision for technology cooperation. Several senior White House officials worked on technology collaboration frameworks before joining the administration, and early reporting indicates that they will adopt a flexible approach, organizing variable coalitions of industry-leading countries. However, the specifics remain vague, with the potential scope of such groups ranging from technical standard- and regulatory-setting partnerships, technology-control coordination, alignment of supply-chain management, and more ambitious joint R&D efforts.

The Quad’s emerging and critical technology working group represents the first concrete step toward a “tech alliance,” but it has a much narrower scope than the EU and U.S. proposals. The White House factsheet lists five areas of focus: principles for technology design, development, and use; technology standards development; telecommunications deployment and diversification of suppliers; monitoring critical and emerging technology trends and opportunities; and critical technology supply chains. At this point, the action items are mostly dialogues, and leaders will likely prioritize the Quad’s joint vaccine efforts in the short term.

Q4: What are the roadblocks to deeper cooperation?

A4: Behind all the enthusiasm for cooperation, there are three primary obstacles to a potential “tech alliance”: different interpretations of the challenges posed by China, existing policy irritants, and economic competition among U.S. allies and partners.

While Washington and its allies share anxieties over China’s rise, they view the specific challenges from different perspectives. In his first speech on the Biden administration’s foreign policy vision, Secretary of State Blinken labeled China “the biggest geopolitical test of the 21st century” and recognized that the bilateral relationship “will be competitive when it should be, collaborative when it can be, and adversarial when it must be.” Brussels adopted similar language in its 2019 Strategic Outlook on China, which identified Beijing as simultaneously a cooperation partner, negotiating partner, economic competitor, and systemic rival. Yet the transatlantic powers have prioritized different aspects of the multifaceted relationship, with Brussels concluding a hard-fought comprehensive agreement on investment with Beijing just weeks before Blinken said he agreed with the Trump administration’s determination that the Chinese government is committing genocide in Xinjiang. Other vital partners have been careful not to publicly oppose China. While the readout of recent U.S.-Japan officials’ meetings heavily criticized Beijing’s behavior, the summary of U.S.-Korea meetings the following day did not mention China.

Existing policy disputes and differences, if left unresolved, will also hinder efforts at cooperation. The European Commission’s Trade and Technology Council agenda urges resolution of “bilateral trade irritants,” referring to U.S. national security tariffs on European steel and aluminum and retaliatory duties over subsidies to Boeing and Airbus. A greater test for policymakers lies with reconciling divergent visions of data governance and competition policy, which will shape the nature of emerging technology development.

Finally, while allies share strategic interests, they are also fierce economic competitors. Countries in a potential tech alliance are racing with each other to lead in emerging technologies, with large public investments in batteries, artificial intelligence, and semiconductor manufacturing capacity, among others. Such efforts could be interpreted as discriminatory industrial policy; Brussels has already voiced concerns that recent “Buy American” initiatives could violate World Trade Organization rules.

While these challenges are significant, they are not insurmountable. Views of China have been converging across key U.S. technology partners, albeit at different speeds. There have been positive early indications from the Biden administration that it is willing to compromise on long-standing U.S.-EU irritants, such as a global digital services tax and the Boeing-Airbus dispute. Going forward, how the Biden administration approaches data governance and builds out its “Buy American” program could determine whether deeper allied technology cooperation is possible.

### 2AC — No Solvency and No Quad Net-Benefit

#### No Solvency and No Quad Net-Benefit — can’t solve tech innovation, China balancing, or deterrence.

Menon 21 — Rajan Menon, Emeritus Anne and Bernard Spitzer Chair in Political Science at the City College of New York/City University of New York, Senior Research Fellow at the Saltzman Institute of War and Peace Studies at Columbia University, Global Ethics Fellow at the Carnegie Council on Ethics in International Affairs, former Monroe J. Rathbone Professor and Chairman in the Department of International Relations at Lehigh University, former Fellow at the New America Foundation, former Senior Fellow at the Council on Foreign Relations, former Special Assistant for Arms Control and National Security to Congressman Solarz, holds a Ph.D. in Political Science from the University of Illinois at Urbana-Champaign, 2021 (“The Quad Is a Delusion,” *Foreign Policy*, June 28th, Available Online at https://foreignpolicy.com/2021/06/28/quad-delusion-china-power-containment/, Accessed 07-17-2022)

One specific facet of U.S. China policy that also blurs the Trump-Biden distinction is strengthening the Quadrilateral Security Dialogue, known as the Quad. Comprised of the United States, Australia, India, and Japan, it emerged in 2007 as a brainchild of Japanese Prime Minister Shinzo Abe and held its first summit this March, after which its members issued a joint statement. Following the conclave, U.S. Secretary of State Anthony Blinken and U.S. Secretary of Defense Lloyd Austin traveled to northeast Asia to maintain the momentum. Austin also added India to his itinerary. Chinese officials promptly lambasted the Quad as the real threat to peace and even warned smaller Indo-Pacific countries—Bangladesh for one—not to cooperate with it, essentially repeating the message it delivered to the Association of Southeast Asian Nations (ASEAN) last fall.

The Quad’s emergence shouldn’t surprise Beijing. Rising powers routinely evoke countervailing coalitions, and shared anxiety about an adversary can contribute to their cohesion—but that’s just a starting point. The Quad’s problem is it doesn’t have much else to run on and hence will ultimately amount to U.S. power with a multilateral veneer.

Of the Quad’s members, only the United States can maintain a sizeable, strong, and enduring military presence in the East China Sea and the South China Sea, the most likely venues for confrontation with China. The U.S. military has power projection forces, sea-based air support, surface ships and submarines, and regional bases to support deterrence and warfighting. Beijing’s nuclear weapons may serve as instruments of coercion against Japan and Australia, perhaps even nuclear-armed India, but won’t be credible against the United States, which has many more of them than China does.

In a nonnuclear clash with China, something no sane person should want, the United States might win, or at least end the war, on favorable terms (although war games suggest otherwise). But even if it could narrowly prevail, in the last few decades, the People’s Liberation Army has acquired the muscle needed to ensure the United States pays a heavy price in the event of a war; and this trend will continue. The United States will nevertheless remain a formidable adversary for China, but the relevant question here is what the rest of the Quad can bring to the table. Not much, hype notwithstanding.

For example, in one standard measure of power, India’s population nearly equals China and because of a higher fertility rate will soon surpass it. Although population size can be an asset, much depends on the human capital developed with it. Unfortunately for India, on that score, China is by most measures—longevity, levels of education, technical skill, caloric intake, and health—far ahead. Ditto for technology, where the gap will grow: Not only does China’s GDP exceed India’s by a factor of four, but Beijing devotes 2 percent of its GDP to technological research and development compared to India’s 0.7 percent. On private, governmental, and university research and development combined, India spends nearly $48 billion annually and has 156 million researchers per million people. The equivalent sums for China are $346 billion and 1,089 researchers. Compare the two countries in internet availability; the quality of schools, universities, and infrastructure; and achievements in cutting edge technologies (robotics, artificial intelligence, 5G, and supercomputers—of which China has nearly twice as many as the United States), and China’s overwhelming edge becomes apparent again.

These differences help explain China’s clear advantages over India in power projection and quality of armaments as well as reconnaissance, target acquisition, and cyberwarfare systems. And because of its overall technological superiority and a military budget almost four times bigger than India’s, China will maintain and even increase its lead. Moreover, Indian forces must travel more than 2,350 miles to reach the South China Sea while Chinese troops sit atop India’s vast northern frontier. So it’s hard to imagine precisely how India can help the United States deter, let alone defeat, China.

Perhaps no East Asian country (leaving aside Taiwan) worries more about China’s resurgence than Japan for obvious historical and geographical reasons. Yet Japan has some big advantages compared to India. Although Japan’s GDP is less than 40 percent of China’s, it still ranks third in the world and is 2.5 times greater per capita. The quality of Japan’s human capital is superb, and it is also a front-rank technological power with a vast pool of skilled labor and scientific expertise.

As for the military side of the ledger, Japan’s Self-Defense Forces are technologically advanced, and critical assessments conclude its sophisticated defense industries produce world-class high-tech armaments. Yet China spends five times as much on the People’s Liberation Army, which has many more weapons essential to success in war. China’s leaders also have pushed military modernization relentlessly, and although Japan has increased its defense budget for nine successive years, military spending has been less than 1 percent of GDP for nearly 60 years. Tokyo could, in principle, make the political decision to increase this proportion substantially, but there’s no evidence of any such move on the horizon. If Japan opts for continuity and joins an anti-China military coalition in East Asia, it will be taking big risks.

Since Japan’s Treaty of Mutual Cooperation and Security with the United States doesn’t obligate the Self-Defense Forces to help the United States in a war with China regardless of the circumstances (note the wording of Article V), Japan would risk exposure to Chinese missiles and airstrikes if it went beyond its treaty obligations. Not surprisingly, despite Washington’s call for a common front, Tokyo has refused to commit to help defend Taiwan, something Japanese Prime Minister Yoshihide Suga made clear following his April meeting with Biden and despite the reference to Taiwan (an anodyne call for “peace and stability across the Taiwan Strait”) in their joint statement. U.S. officials were doubtlessly disappointed, but given strategic realities, why would Japan roll the dice when it can count on U.S. protection without doing so?

Australia, the Quad’s fourth member, can’t really beef up the group either. Its navy must sail more than 3,000 miles to reach the South China Sea, 500 miles more to get to Taiwan. Once there, it would have to contend with China’s missiles, submarines, and aircraft as well as Chinese operations aimed at severing the sea lines of communication supplying Australian forces. True, Australian warships have sailed the South China Sea since World War I, but in the last few decades, China, no longer weak, has transformed the local balance of power. Although Australian naval vessels joined U.S., Indian, and Japanese ships for the Malabar exercises (which started in 1992) on two occasions—2007 and 2020—Australia’s navy lacks the punch to ensure maritime missions against China are something other than a U.S. undertaking. The apparent enthusiasm of Campbell and U.S. National Security Advisor Jake Sullivan for a more expansive Australian naval strategy won’t change that. Although Australians increasingly distrust China and consider it a threat, in a recent Lowy Institute poll, 57 percent wanted Australia to stay out of any Sino-American conflict.

Perhaps it’s wrong to judge the Quad in purely military terms; after all, strategy doesn’t reduce solely to brute force. Yet a wider view doesn’t change the overall picture. If the Quad is also to be a political partnership aimed at countering China’s growing influence in East Asia, what exactly will its members do to achieve that goal, and what will be the division of labor? How will the Quad overcome ASEAN’s evident reluctance to get sucked into the intensifying rivalry between China and its adversaries? Perhaps the United States’ Quad partners could help exert economic pressure on Beijing, but given their dependence on Chinese trade and investments as well as vulnerability to retaliation, it’s hard to see them doing that except episodically and delicately. Australia, 39 percent of whose exports go to China compared to less than 4 percent to the United States, has already experienced such blowback after it banned Chinese telecommunications giant Huawei from 5G projects, criticized Beijing’s behavior in Hong Kong and Xinjiang, and called for investigating the origins of COVID-19. China imposed multiyear tariff hikes on key Australian exports, including wine (more than 200 percent) and barley (80 percent). Moreover, rock lobsters—96 percent of which was exported to China—were blocked by inspections; several meat producers were shut out; and ships carrying coal, barred from offloading their cargo, were stranded for months. Australia didn’t cave, but Beijing didn’t expect that. Its goal was to send a message—not just to Canberra.

The Quad won’t disappear; it will hold summits, issue statements, and stage naval exercises. But those who want it to become central to Washington’s neo-containment strategy are deluding themselves.

### 1AR — No Quad Net-Benefit

#### The Quad can’t counter China — other members won’t take sides.

DePetris 21 — Daniel R. DePetris, Fellow at Defense Priorities, Middle East and Foreign Policy Analyst at Wikistrat, Inc., Researcher at the Southwest Initiative for the Study of Middle East Conflicts, Columnist at the *National Interest*, *The American Conservative*, *The Huffington Post*, and *The Washington Examiner*, holds an M.A. in Political Science from the Maxwell School of Citizenship and Public Affairs at Syracuse University, 2021 (“Biden should be aware of the limits of the Quad,” *The Hill*, September 27th, Available Online at https://thehill.com/opinion/international/574023-biden-should-be-aware-of-the-limits-of-the-quad/, Accessed 07-18-2022)

Australian Prime Minister Scott Morrison, Japanese Prime Minister Yoshihide Suga and Indian Prime Minister Narendra Modi received the red-carpet treatment at the White House last week for the first in-person meeting of the Quadrilateral Security Dialogue. President Biden’s decision to host the summit comes about six months after the Quad released a joint leaders statement pledging to “commit to promoting a free, open rules-based order” in the Indo-Pacific region.

For Biden, the leaders’ summit is a golden opportunity to elevate a broad theme of his presidency: utilizing international partnerships to manage the challenges of the 21st century, in particular China’s quest to become Asia’s dominant power. But if the Biden administration seeks to turn the Quad into an anti-China balancing coalition or, more dramatically, a new NATO in Asia, it will be setting itself up for disappointment. While Australia, Japan and India all have strong disagreements with China and are growing increasingly concerned about Beijing’s behavior in the region, none of these countries seem especially interested in allowing Washington to dictate its policy in Asia. Unlike Washington, the Japanese, Indians and Australians live in the Indo-Pacific and have to be especially careful before rocking the boat with Beijing.

As China’s economic and military strength grows, the nation is getting more assertive as it moves to protect its own interests. Last year, Chinese naval vessels sailed in the waters of the Japanese-administered Senkaku islands for 333 consecutive days, deployments that continue to test Tokyo’s defensive measures and response time. Japan’s Defense Ministry, in its most recent annual white paper, stressed that “Chinese military trends…have become a matter of grave concern to the region.” India, meanwhile, is still facing off with tens of thousands of Chinese soldiers on the other side of its disputed Himalayan border, where there were clashes last year. China is also continuing its campaign of economic pressure against Australia, adopting tariffs and import restrictions on everything from Australian wine and barley to coal and seafood.

These problems aside, Australia, Japan and India recognize their friction with China would get even worse should they use the Quad as a vessel to confront Beijing. This is especially true in New Delhi, which is careful to avoid picking sides between the world’s two greatest powers. Historically paranoid about U.S. security promises, India is following a path of multi-alignment, which encourages the improvement of relations with as many countries as possible in order to preserve flexibility, keep its options open, and retain freedom of movement in a tricky region of the world. For India to follow Washington’s lead or throw its weight fully in the U.S. camp would rip that doctrine apart. It would also have dangerous economic consequences for India at a time when its trade relationship with China has reached record levels ($57.48 billion) in the first quarter.

Japan has longstanding territorial arguments with Beijing and is no doubt becoming more outspoken about Taiwan, perhaps China’s most sensitive issue. The Japanese defense budget has also gotten larger every year for the last nine straight years, driven in large part by China’s saber-rattling. Yet just because the Japanese are purchasing more F-35’s, long-range missiles and warships doesn’t mean Tokyo is looking for a fight — especially a fight that would jeopardize the very export markets that undergird Japan’s $5 trillion economy. With China consuming more than 20 percent of Japan’s total exports last year, Tokyo’s limitations are quite real.

Australia is arguably the one member of the Quad that may be sympathetic to using the multilateral forum to push back against China. Canberra clearly had China in mind when it decided to opt-out of a diesel-powered submarine deal with France in favor of U.S. and British nuclear propulsion technology. While senior Biden administration officials were insisting that the new AUKUS security pact between the U.S., the U.K. and Australia wasn’t about any one country, Australian Foreign Affairs Minister Marise Payne all but stated openly that China’s behavior was the genesis of the arrangement.

Even so, Australia isn’t in the position to compete with China militarily — certainly not without substantial U.S. military and logistical assistance. The South China Sea is roughly 3,000 miles away from Australia, which means the Australian navy would need to go to extraordinary lengths just to become a serious contributor to a hypothetical anti-China military coalition. The economics of such a decision wouldn’t be lost on the Australian government; at $245 billion, China accounted for 31 percent of Australia’s total trade last year. If China was willing to levy trade restrictions in retaliation for Australia’s call for an international investigation into the coronavirus pandemic, it’s not difficult to envision Beijing taking even more strident action against the Australian economy if Canberra outsourced its China policy to Washington.

None of this is to argue that the Quad is useless. To the extent common interests bind the United States, Australia, Japan and India together, a regional forum such as the Quad can be a force multiplier, providing all four nations with the opportunity to collaborate and sync their approaches. But Biden would be wise to avoid transforming this multilateral club into a formal security alliance. The other members aren’t interested in choosing sides. And Washington shouldn’t force them to do so.

#### Economic interdependence with China prevents Quad balancing.

Chowdhury 21 — Debasish Roy Chowdhury, Hong Kong-based Editor and Author specializing in Asian current affairs with a focus on India, former Senior Research Fellow at the Sydney Democracy Network at the University of Sydney (Australia), former Deputy China Editor at the South China Morning Post, holds an M.A. in Economics, 2021 (“Quad is Key to Biden's Strategy in Asia, But the Four-Way Alliance Is Ambiguous and Contradictory,” *Time*, March 18th, Available Online at https://time.com/5947674/quad-biden-china/, Accessed 07-18-2022)

The clarity with which Biden is mending fences with traditional allies is commendable. But the same can’t be said of the fancy new Asian mega alliance touted as the centerpiece of his Asia play. Biden has cemented an informal grouping of four maritime democracies in the Indo-Pacific region. After over a decade of dithering, the leaders of the U.S., Australia, Japan and India summitted for the first time—albeit virtually—as a strategic bloc last week. The so-called Quadrilateral Security Dialogue, or Quad, is supposedly an Asian Nato that will act as a bulwark against a rising and assertive China. But its confusing alliance logic, foundational contradictions and deliberate ambiguity make it more like that king of multilateral duds, BRICS (Brazil, Russia, India, China and South Africa)—a grouping of nations with nothing in common besides an acronym plucked out of a Goldman Sachs report.

The hype aside, Quad in reality bears no resemblance to Nato. The latter represented a grand strategy of culturally similar Western nations with a mutual history of trust and cooperation forged through conflicts and crises. Nato countries equally shared a perception of Moscow as a threat, resulting in a clear strategy of countering and containing the Soviet Union. Zero commercial entanglement between Nato and the insular Soviet bloc made the goal of containment an uncomplicated exercise.

Contrast that with Quad, or even the broader Indo-Pacific region, where all countries share critical economic interdependence with China. China is Japan’s largest export market and trading partner, representing more than a fifth of Japan’s total trade. China is also the largest trading partner of Australia, accounting for about 30 percent of Australia’s trade with the world. Nearly 40 per cent of Australian goods exports go to China, which in turn supplies 27 percent of all goods imported into Australia. Even for India, which has a live boundary dispute with China that flared up in a bloody conflict in the Himalayas last year, China is the largest trading partner. Total imports from China are more than India’s combined purchases from the U.S. and the U.A.E., its second and third largest trade partners.

Intertwined economic interests, along with the risk of a Chinese blowback to perceived encirclement, meant Quad never quite took off after it was established in 2004 as an ad hoc group to deal with the devastation of the Boxing Day tsunami. Championed by Japanese leader Shinzo Abe, it had its first meeting in 2007 as an informal strategic group. The on-again, off-again Quad was revived by the Trump administration in 2017, after a decade in cold storage, as tensions between China and its neighbors mounted. But the old hesitancy lingers.

A joint statement was issued after the members met last Friday but it made no mention of China—the very reason why the group supposedly exists. A joint op-ed issued by the four leaders similarly danced around the inconvenient topic of China, focusing instead on COVID-19, vaccines, climate change and assorted generalities such as “challenges presented by new technologies.”

This week, while visiting Tokyo, Secretary Bilken warned China against using “coercion and aggression.” But the U.S. is an exception. Other Quad members avoid attacking China directly, or even naming it as an adversary, lest it offends Beijing. As a group, they take pains to make the point—unconvincingly—that Quad is not aimed at any one state. They use phrases like “rules-based regional order” and “shared challenges” as codes to refer to China. But it begs the question of how one tackles a problem if it can’t even be plainly identified or isn’t pressing enough to rally against unequivocally. It is also not clear why countries like Vietnam, the Philippines and Indonesia have stayed away from Quad if a united front against a domineering China is really the need of the hour for Asia.

Unclear too is the emphasis on “democratic values” as Quad’s binding ethos. Using democracy as the basis for alliance in one region sits at odds with America’s partnerships in other parts of the world, notably the Middle East. The Quad summit, which came close on the heels of a considered decision by Biden not to order action against Saudi Crown Prince Mohammed bin Salman for his murderous ways, only highlighted this duality.

The contradictions don’t end there. Even within the Indo-Pacific region, well-entrenched democracies like South Korea and New Zealand are outside Quad. India, on the other hand, is a key member because its blue-water naval capacity outweighs its increasingly shallow democratic credentials. Assaults on civil liberties, political rights and minorities have increased noticeably in recent years under the watch of Prime Minister Narendra Modi’s Hindu nationalist government. Only a day before the Quad summit, Sweden’s V-Dem Institute, which tracks rights and democracies worldwide, declared in its latest report that India had turned into an “electoral autocracy”. Earlier in the month, US-based non-profit Freedom House downgraded India from a free democracy to a “partly free” country. The presence of a country with rapidly shrinking freedoms doesn’t do credit to a bloc supposedly founded on democratic values and demanding a “free, open and inclusive Indo-Pacific.”

How an ill-defined intergovernmental grouping with credibility issues and devoid of a clear mandate is perceived by the Chinese will become evident as National Security Adviser Jake Sullivan and Secretary Blinken meet their Chinese counterparts Yang Jiechi and Foreign Minister Wang Yi this week in Anchorage, Alaska for a new round of formal talks between the two estranged powers. Quad may give the Biden Administration a strong hand in the negotiations—if Beijing accepts the alliance as proof of Washington’s ability to still lead in Asia. But beyond that, it’s difficult to see how the quadrilateral is square with Asia’s needs.

#### Only formal collective defense via NATO can counter China.

Holmes 20 — James R. Holmes, J. C. Wylie Chair of Maritime Strategy at the U.S. Naval War College, former Faculty in the School of Public and International Affairs at the University of Georgia, former Surface Warfare Officer in the U.S. Navy, holds a Ph.D. in International Relations from the Fletcher School of Law and Diplomacy at Tufts University, 2020 (“The Quad Is An Important Partnership, But It Is Not NATO,” *The National Interest*, August 30th, Available Online at https://nationalinterest.org/blog/reboot/quad-important-partnership-it-not-nato-192783, Accessed 07-18-2022).

**[\*\*\*Note: This article was probably published in 2020. The date listed is 2021, but there is a note at the bottom that says “This piece first appeared last year and is being republished due to reader interest.” *The National Interest* does this frequently and it is often confusing.\*\*\*]**

China grumps that the Quad, a league of like-minded Indo-Pacific democracies, is an “Asian NATO” or “mini-NATO” hellbent on “containing” China.

If only.

Now, Beijing is not entirely wrong to liken the Quad to the North Atlantic Treaty Organization. Quad governments—representing India, Australia, Japan, and the United States—sometimes do things reminiscent of the Atlantic alliance. For instance, the four Quad navies just finished up with this year’s Malabar exercise in the Arabian Sea, showing they can work together and push back as China tries to make itself a serious if not dominant player in the Indian Ocean region. NATO navies commonly maneuver together, casting a counterweight to Russian ambitions in the Atlantic Ocean and adjacent seas.

But one of these things is not like the other. In reality, the Quad is a loose consortium, not a standing alliance anchored by a collective defense treaty. The arrangement bears more resemblance to the pre-World War I “entente cordiale” than to NATO. In April 1904 the French and British governments signed a series of agreements settling long-standing colonial quarrels. Setting aside centuries of on-again-off-again enmity, the two democracies drew together against the common danger manifest in autocratic Germany.

Kaiser Wilhelm II and his lieutenants repeatedly sought to break the entente in ensuing years, yet their bellicose diplomatic methods only cemented it. French ally Russia ultimately joined in, and the “Triple Entente” was on. As a result, a coalition—not a formal alliance—squared off against imperial Germany and its allies in 1914. Pre-war European alliance politics should come as cold comfort to Beijing. It shows that an overbearing power can prompt its opponents to make a common cause even when no mutual defense accord binds them to do so.

It also shows they can win.

NATO itself is something of an anomaly, as indeed is the array of alliances the United States has headed since 1945. Namely, the protracted strategic competition known as the Cold War lurched into being during the immediate aftermath of a system-shattering global war. The victorious World War II allies fell out against one another in the months after peace came. The Iron Curtain descended across Europe while America sought to rally the noncommunist world to oppose Soviet expansionism.

The anomaly is this. U.S. forces were already on the ground in war-stricken parts of the world, helping enforce the peace and reconstruct devastated countries. Allies did not invite America to construct and garrison bases on their soil during peacetime. That would have been a tough sell with host governments and peoples. U.S. forces came as conquerors; they stayed to hedge against fresh aggression. Facts on the ground simplified the challenge of forging Cold War alliances.

In a real sense, then, U.S. containment strategy was an artifact of World War II.

Lord “Pug” Ismay, the first secretary-general of NATO, encapsulated the alliance’s rationale breezily but accurately: its reason for being was to keep the Russians out, the Americans in, and the Germans down. Keep being the keyword. The Americans were already in; they did not have to be invited in. That made it politically easier for allied governments to ask them to stay, helping keep the Soviets behind the Iron Curtain and hold down new militarism in Germany.

The American presence was the status quo—not some radical break from the status quo. And it’s easier to defend an established status quo than to disturb one.

Similar logic held in Asia, where the defeat of Japan splintered the Japanese Empire into its constituent parts, many—including Japan itself—under direct U.S. military occupation. The U.S.-Japan security alliance was a kind of bilateral NATO meant to keep the Russians and Chinese out, the Americans in, and the Japanese down. South Koreans didn’t need to be kept down. After being ravaged by World War II and the Korean War, though, they consented to a strong U.S. military presence to keep North Koreans and their communist backers out and Americans in.

Lord Ismay’s quip furnishes a powerful instrument for evaluating U.S.-led alliances past, present, and future. That instrument indicates that the Quad stands apart from long-standing alliances. The United States is not an occupying power in Quad members. Its presence in Japan long ago evolved into a mutual arrangement. Indeed, the U.S.-Japanese duo is more an alliance of equals by the day.

Australia is arguably America’s closest friend on the planet yet remains reluctant to permit a standing presence that might entangle Canberra in adventures it prefers to avoid. The Australian government does allow U.S. Marine contingents to deploy to the northern harbor of Darwin on a rotating basis. Still, the situation bears scant resemblance to Europe or East Asia during the early Cold War.

And India? Fuggedaboutit. New Delhi pioneered nonalignment during the Cold War. It had an occasionally fraught relationship with the United States (and a cozy one with the Soviet Union) whose legacy the partners are only now transcending. And a tradition of autonomy is etched on Indian strategic culture. India regards itself as a benign hegemon over the Indian Ocean region. No hegemon readily submits to an alliance headed by outsiders, let alone allows outsiders to establish a standing military presence on its territory. Only under extreme duress would New Delhi break with strategic autonomy.

The Quad is no NATO.

### 2AC — Counterplan Decreases Quad Credibility

#### Counterplan Decreases Quad Credibility — pushing it to more aggressively challenge China alienates everyone else in the region.

Feigenbaum and Schwemlein 21 — Evan A. Feigenbaum, Vice President for Studies at the Carnegie Endowment for International Peace, Practitioner Senior Fellow and former James R. Schlesinger Distinguished Professor at the Miller Center of Public Affairs at the University of Virginia, former Deputy Assistant U.S. Secretary of State for Central Asia, holds a Ph.D. in Chinese Politics from Stanford University, and James Schwemlein, Nonresident Scholar in the South Asia Program at the Carnegie Endowment for International Peace, former Senior Advisor to the U.S. Special Representative for Afghanistan and Pakistan at the U.S. Department of State, holds an M.A. in International Affairs from American University, 2021 (“How Biden Can Make the Quad Endure,” Carnegie Endowment for International Peace, March 11th, Available Online at https://carnegieendowment.org/2021/03/11/how-biden-can-make-quad-endure-pub-84046, Accessed 07-18-2022)

Avoiding the China Trap

The bottom line is this: to endure and meaningfully solve problems, the Quad needs to shift its focus from its novel form of dialogue toward joint functional action by the group on the most pressing priorities that others in the region now face. If other countries in Asia view the Quad as little more than a talk shop to discuss the looming risks posed by China’s rise while occasionally holding joint military exercises, it is unlikely that other countries will see its utility or view it as a model for their own choices and conduct.

Of course, Beijing’s actions toward Australia and India over the last year highlight the benefits of solidarity among like-minded partners. But the rest of Asia is less focused on the Quad’s problems with Beijing and the security dimensions of its partnership than on grappling with an array of daily challenges and pressing, long-term development priorities. To lead, the Quad countries must demonstrate in deed, not just word, that they are making major contributions to solving the larger economic, transnational, and environmental challenges that preoccupy nearly everyone else in the Indo-Pacific.

If it does so successfully, the Quad can comprise the firm core of an elastic regional architecture. Ultimately, the priority today should not be on countering China for its own sake but on increasing areas of alignment and cohesion with a larger community of potential problem-solving partners. That is the best path for advancing the interests of the Quad countries, preserving security, and promoting development in the Indo-Pacific.

## AT: Trilateral India-Israel-U.S. CP

### 2AC — Indian Innovation Fails

#### Indian Innovation Fails — multiple problems.

Behera 21 — Laxman Kumar Behera, Associate Professor in the Special Centre for National Security Studies at Jawaharlal Nehru University (India), former Core Member of the Defence Economics and Industry Centre of the Institute for Defence Studies and Analyses (India), holds a Ph.D. in International Relations and National Security Studies from Jawaharlal Nehru University (India), 2021 (“Examining India’s defence innovation performance,” *Journal of Strategic Studies*, Volume 44, Issue 6, Available Online to Subscribing Institutions via Taylor & Francis Online)

Abstract

India has expended a great deal of energy and resources to set up a vast defence economy to innovate state-of-the-art weapon systems. However, the performance of the defence economy has been largely suboptimal. An examination of the causes of poor performance exhibits a number of shortcomings related to India’s both ‘hard’ and ‘soft’ innovation capacities. Lack of strong support from higher political leadership, meager research and development (R&D) and procurement budgets, inefficiency of the main R&D and manufacturing players, poor management of human resources and a weak acquisition system, among others, leave India’s defence innovation in a poor state.

### 1AR — Indian Innovation Fails

#### India’s defense innovation is weak.

Behera 21 — Laxman Kumar Behera, Associate Professor in the Special Centre for National Security Studies at Jawaharlal Nehru University (India), former Core Member of the Defence Economics and Industry Centre of the Institute for Defence Studies and Analyses (India), holds a Ph.D. in International Relations and National Security Studies from Jawaharlal Nehru University (India), 2021 (“Examining India’s defence innovation performance,” *Journal of Strategic Studies*, Volume 44, Issue 6, Available Online to Subscribing Institutions via Taylor & Francis Online)

Conclusion

Barring a few successes especially in missile and other strategic programmes and warship building, India’s defence innovation performance can at best be described as lacklustre. This is amply evident from India’s continued high import dependency for major conventional arms, apart from poor component level innovation. The poor innovation performance can be attributed to a number of factors, related to both hard and soft innovation capabilities.

### 2AC — Status Quo Solves India-Israel-U.S. Alliance Net-Benefit

#### Status Quo Solves India-Israel-U.S. Alliance Net-Benefit — recent symbolic and material commitments are sufficient.

Magid 22 — Jacob Magid, U.S. Correspondent at *The Times of Israel*, 2022 (“Israel, India, US, UAE unveil joint food security, energy projects at virtual summit,” *The Times of Israel*, July 14th, Available Online at https://www.timesofisrael.com/israel-india-us-uae-unveil-joint-food-security-energy-projects-at-virtual-summit/, Accessed 07-15-2022)

The leaders of Israel, India, the United States and the United Arab Emirates announced on Thursday a pair of massive collaborative projects in the fields of food security and clean energy after they met at a virtual summit during US President Joe Biden’s visit to Jerusalem.

Biden, Prime Minister Yair Lapid, UAE President Mohamed bin Zayed and Indian Prime Minister Narendra Modi made the announcement in a joint statement their offices issued during their virtual meeting — the highest-level gathering to date of the new, US-formulated I2U2 forum.

In public remarks before the closed-door meeting, the four leaders stressed the importance of working together to address global challenges.

“We need to think in new terms when it comes to energy, food security, water tech, defense and trade,” Lapid said. “In the 21st century, challenges are local but solutions are global.”

The Israeli premier highlighted the food security crisis in the wake of Russia’s invasion of Ukraine, calling the emerging food corridor between India and the UAE “a clear example of a solution to a problem we are all facing.”

Speaking after Lapid, Biden said the meeting is “about demonstrating the importance of showing the practical impacts” of Israel’s growing integration.

“Our challenge together is to deliver real results that people can feel in their everyday lives,” he continues. “We can do a great deal if we stick together,” the president concludes, stressing that he intends to stay engaged on the matter.

“Under the I2U2 framework, we have agreed to increase joint investment in six important areas: water, energy, transport, space, health and food security. It is clear that both the vision and agenda of I2U2 are progressive and practical,” Modi said.

“I also hope that our quartet will be a model for those who desire peace and prosperity,” bin Zayed said.

US National Security Adviser Jake Sullivan told reporters en route to Israel on Wednesday that bringing together Israel, India and the UAE, particularly to utilize their expertise to address food security challenges, fulfills Biden’s vision of a “more integrated, more globally engaged Middle East.”

“We think I2U2 can become a feature of the broader region, just as the Quad has become a central pillar of the Indo-Pacific strategy of the United States,” Sullivan said, referring to the security dialogue the US has with India, Australia and Japan.

Thursday’s joint statement said the four countries would aim to “harness the vibrancy of our societies and entrepreneurial spirit to tackle some of the greatest challenges confronting our world, with a particular focus on joint investments and new initiatives in water, energy, transportation, space, health and food security.”

The I2U2 countries also will utilize their respective private sectors to advance low carbon development pathways, improve public health and access to vaccines, jointly create new solutions for waste treatment, and promote the development of green technologies, the communique said.

The countries stressed their support for Israel’s integration in the region, drawing a connecting line between the Abraham Accords normalization agreements and the formation of forums such as the I2U2. They also welcomed other new regional groupings such as the Negev Forum, which consists of Israel, the UAE, Bahrain, Morocco, Egypt and the US.

Notably, the joint statement made no mention of the Palestinians. The US in the past has pressed for the inclusion of a commitment to advance the two-state solution in such documents, though it might have been outnumbered by the three other countries whose leaders have expressed less interest in publicly promoting the issue.

The leaders “discussed innovative ways to ensure longer-term, more diversified food production and food delivery systems that can better manage global food shocks,” the communique said.

As for the two projects announced Thursday, the first will see the UAE invest $2 billion to develop a series of food parks across India that will incorporate green technologies to reduce food waste, conserve fresh water and employ renewable energy sources.

The collaboration will see India provide land and integrate its farmers into the project, and the US and Israel will encourage their respective private sectors to offer their expertise for the initiative, which will help address food insecurity in South Asia and the Middle East.

The second initiative will be the creation of a hybrid renewable energy project in “India’s Gujarat State of 300 megawatts (MW) of wind and solar capacity complemented by a battery energy storage system,” the joint statement said.

The US Trade and Development Agency footed the bill for a $330 million feasibility study for the project and Emirati companies are exploring investment opportunities, with the encouragement of the US and Israeli governments. The project will help advance India’s goal of achieving 500 GW of non-fossil fuel capacity by 2030 and transforming the country into a global hub for renewable energy.

The I2U2 leaders stressed that the two projects were only the beginning of a “long-term strategic partnership that… improve the movement of people and goods across hemispheres and increase sustainability…[through] collaborative science and technology partnerships.”

### 2AC — No India-Israel-U.S. Alliance Net-Benefit

#### No India-Israel-U.S. Alliance Net-Benefit — competing foreign policy interests make trilateral defense cooperation impossible.

Kamal 22 — Hassan M. Kamal, Assistant Editor at the Associated Broadcasting Company (India), 2022 (“Explained: Why the new grouping I2U2 is not a West Asian Quad,” *News 9*, July 14th, Available Online at https://www.news9live.com/world/explained-why-the-new-grouping-i2u2-is-not-a-west-asian-quad-182479, Accessed 07-15-2022)

For the India-Israel-UAE-US alliance to be equated with the Quad, the I2U2 bloc must agree to work together on defence and security, which seems unlikely given the members' competing interests.

The heads of states of India, Israel, the UAE and the US will come together for the first virtual summit of a new bloc known by the moniker I2U2 today. The 'I' stands for Israel and India while the 'U' stands for the UAE and the US.

Prime Minister Narendra Modi, Prime Minister of Israel Yair Lapid, President of the UAE Sheikh Mohamed bin Zayed Al Nahyan and US President Joseph R Biden will take part in the meeting. Modi and Sheikh Mohammed will attend the summit virtually while Biden and Lapid will be physically present for the meeting.

The I2U2 grouping was conceptualised during the meeting of the foreign ministers of the four countries held on October 18, 2021.

The group has emerged as the talking point amid changing global politics. The participating nations have termed it a purely economic group with focussed cooperation in six mutually recognised areas such as water, energy, transportation, space, health, and food security. However, some experts have dubbed the meet as West Asia 'Quad', despite the fact that existing geopolitical realities work against such nomenclature. Here's why:

Disagreement over Iran, China and Russia

In the ever-changing global politics where national interests seem to be the driving factor of foreign policy, the I2U2 comes across as a collection of unlikely countries whose current foreign policies, if continued, will create divisions rather than unify them. Among the many key foreign policy issues that divide the group are how to deal with Russia, China and Iran.

The Russia question: Though the US has reiterated that the global food crisis in the backdrop of the Ukraine conflict is going to be one of the main topics of the I2U2, the US is likely to find itself isolated in convincing the other members that Russia is behind the global food crisis.

Apart from the US, none of the other three countries in the I2U2 — Israel, India and the UAE — have followed the Western steps in imposing sanctions on Russia. In fact, they have continued to maintain "good" ties with Moscow. India specifically has increased its oil purchases to tide over the high fuel prices. India has also abstained from voting on either UN or UNSC resolutions against Russia.

Israel, in the meanwhile, has refused to sell its Iron Dome System to Ukraine to protect Ukrainian cities and military establishments from Russian attacks despite US approval.

The UAE, too, has abstained from voting against Russia in the UNSC resolutions and has even welcomed Russian oligarchs in the country.

The China Question: The US and India, who are members of the Quad Security Dialogue, a grouping dubbed as an anti-China alliance, are bringing two important nations of West Asia — Israel and UAE — to form a unique West Asian bloc. However, while the Quad's primary objective is to work for a "free, open, prosperous and inclusive Indo-Pacific region," the I2U2 focus is limited to economic collaborations in areas such as water, energy, transportation, space, health, and food security.

The chances of any collaborations in terms of defence and security, which would qualify to term the bloc as a West Asian 'Quad' seem nil. The UAE is already a part of China's Belt and Road Initiative (BRI) while Israel has been benefitting from the ban on US tech imports to China. It also hopes to benefit from the BRI and act as a connecting point between Europe and Asia. So, neither the UAE nor Israel stands to benefit from any efforts at containing China's influence in the region.

The Iran question: Israel says India will strengthen the impact of the Abraham Accords, but it has also made it clear that it is against Iran. The two countries are involved in a proxy war for decades with Iran supporting the Palestine Movement. The Abraham Accords, on the other hand, are a worry for Iran as it has reduced the distance between the Israeli Army and the Iranian border. The accords also allow other West Asian nations to purchase American weapons they couldn't access earlier.

Iran's proxy war against the UAE and Saudi Arabia is also a known fact. Both the UAE and Saudi Arabia, who are friends with India, regularly face drone attacks by Iran-backed Houthis in Yemen.

Despite the complexities of the region, India has managed to maintain good ties with West Asian countries, especially Iran. New Delhi is unlikely to break those ties and join an alliance against Tehran. And for good reasons.

India breaking ties with Iran will benefit China, which has signed a 25-year cooperation deal with Tehran. It would also mean New Delhi abandoning investments in the Chabahar port and other infrastructure projects.

The eastern section of the North-South corridor in Iran connecting Russia to India via Iranian rail has become operational. The first rail transit carrying 39 containers from Russia reached Iran on Tuesday. According to a report in Tehran Times, the cargo will be transported to Bandar Abbas port in southern Iran through a 1,600 km rail route to finally be sent to India's Nhava Sheva Port in Navi Mumbai via sea.

India is one of the largest investors in the Iranian oil and gas industry as well. As Talmeez Ahmed, India's former ambassador to Saudi Arabia, recently told PTI, "There is no way India will join an alliance against Iran."

### 2AC — Pakistan DA

#### Pakistan DA —

#### A. Link — closer India-Israel cooperation on defense innovation causes a security dilemma, accelerates the arms race, and destabilizes South Asia.

Sultaana 21 — Saddaf Sultaana, Ph.D. Candidate in the Strategic Studies Department at the National Defence University (Pakistan), 2021 (“India-Israel Defence Cooperation: Security Implications for Pakistan,” *Journal of Security & Strategic Analyses*, Volume 7, Number 1, Available Online at http://thesvi.org/ojs/index.php/ojs/article/view/131/93, Accessed 07-18-2022, p. 156-160)

India-Israel Defence Ties: Security Implications for Pakistan

The defence and military partnership of India and Israel seems to be enduring because of their mutual strategic interests and continuous collaboration. Israel is facilitating India to acquire requisite defence equipment’s, defence production capability and upgraded weapons to maintain their alliance and sustain its ambition to be a major regional as well as a global power. Sophistication in military technology with the help of Israel and the allocation of high budget for defence purpose indicates that India wants to counter the joint threat of Pakistan and China. Hence, India’s regional and global hegemonic approach and growing defence cooperation with Israel is not only destabilizing the regional strategic balance but also carries severe consequences for the stability of South Asian region. Their clandestine relations during the Cold-War era and strong alliance after the Cold-War period proved to be a potential threat especially for Pakistan’s security. India’s obsession with power projection against strategically compatible Pakistan and strong rival China tempts it to find a reliable defence partner and Israel comes in handy.

In the last two decades, India has strengthened its defence partnership with Israel by pursuing military modernization. Timothy Hoyt writes that “military modernization is most advanced in states which are deeply involved in regional political-military rivalries, or which boast significant military and economic advantage over most of their neighbors. Many developing states face potential external threats, from regional neighbors or outside forces. These threats usually create a demand for advanced military capabilities and an [end page 156] expanded military-industrial base.”79 Therefore, to enhance its operational and deployment capabilities, India is continuously procuring advanced missile defence system, sophisticated delivery mechanism and advanced nuclear technology, which is ultimately raising the “level of threat, insecurity and arms race in the region. Various agreements on missile and defence cooperation with Israel have definitely enhanced military superiority of India while disintegrating the balance of power and compeling Pakistan to allocate extra resources on the defence sector.80 Also, the development in air, naval, satellite and space program has provided India with a strategic gain over Pakistan.

Moreover, the surveillance equipment (i.e., UAVs, cross-border sensors, and Airborne Early Warning” Systems), which India is getting from Israel,81 would help India in carrying out swift and quick operations or strikes against Pakistan and to infiltrate Pakistan’s territory. February 2019 Balakot crisis between India and Pakistan is a recent example that determines the pace of India-Israel defence partnership in which India used Israeli weapons to launch strikes inside Pakistan’s territory.82 Such incident only increases the chances of war between both the states albeit limited, intensify threat matrix for Pakistan and destabilize the peace and stability in the region.” Robert Fisk clearly stated that the defence ties between India and Israel have strengthened in the past few years which include sophisticated training [end page 157] and arms trade. According to him, “Israel has been assiduously lining itself up alongside India’s national BJP government...while India itself has now become the largest weapons market for the Israeli arms trade.”83 Hence, India-Israel strategic and defence partnership is an existential threat to the national security of Pakistan and affecting regional security calculus as well.

For India, who is dreaming to become an “Asian giant,” Israeli military technology and security cooperation provides it with the finest way to cope with its security issues. Governed by geostrategic and geopolitical priorities, the strategic partnership with Israel is enabling India to attain its greatest policy objectives, i.e. to gain regional hegemony. It is being ensured by strengthening its defence sector, to expand its military power beyond its region. The goals are wide-ranging and also include geo-economic objective, blocking Pakistan’s access to and undermine its influence in the Middle East and Central Asian states. It seeks to ultimately destabilize and weaken Pakistan’s defensive balance capability both at the eastern and western front and counter China’s influence in the region. India aspires to annex the illegally occupied Kashmiri territory following Israel’s annexation policy. In short, India-Israel strategic alliance, indeed, is emerging as the major threat to strategic stability “in South Asia and carries far-reaching implications for Pakistan’s security.”

Analyzing the aspects of India-Israel growing proximity and defence ties, it is noted that the strategic equilibrium in the region is shifting in the favor of India. The progression in their relationship not only undermines the military balance of South Asia but also destabilizes the conventional balance vis-à-vis Pakistan. Harsh V. Pant stated that “the [end page 158] most immediate effects of this close defence relationship between India and Israel can be seen in Pakistan’s worry that the strategic balance in the subcontinent is fast tilting against it. It finds it difficult to match the conventional military capability of Israel-India combined.”84 Hence, the conventional and unconventional military superiority of India is helping it to establish hegemony in the region and destabilize Pakistan’s security. Moreover, India and Israel are constantly solidifying their military ties because it is not only India who is apprehensive about the nuclear arsenals of Pakistan, but Israel had also serious concerns about Pakistan’s nuclear weapons program.85 This specifies that India-Israel defence and missile cooperation is not only activating an arms race in South Asia but also destabilizing the deterrence equation besides affecting the strategic stability in the region.

Conclusion

An expansion of defence cooperation between India and Israel along with the acquisition of military and nuclear capabilities by India through its strategic partnership with Israel would not only undermine the regional balance but will also have severe consequences “for the stability of South Asia in future. This cooperation reveals India’s strong commitment to dominance and “power projection in the broader Southern Asian region that includes Indian Ocean and Malacca Straits. Moreover, India considers Pakistan and China a major irritant in its quest for hegemony. Therefore, the defence partnership with Israel is seen as the guarantee to ensuring its ambitions.

All the major arms deal with Israel including the transfer of technology and production of missiles are “part of Prime Minister Modi’s Make in India initiative.” The steady progress and cooperation [end page 159] in missile defence system with Israel under this initiative is generating a regional security dilemma by endangering the security of other states. Development and” acquisition of defence system, as well as missile proliferation, is rigorously undermining the strategic stability and has the potential to accelerate arms race in the region. In this process India seems to have ignored that its actions are worsening the security dilemma, increasing insecurity, intensifying arms race and provoking Pakistan to take countermeasures, which in turn will further deteriorate the security environment of South Asian region.

#### B. Impact — that causes global nuclear war.

Roblin 20 — Sebastien Roblin, 2020 (“Why India-Pakistan's Nuclear Rivalry Is Deadly Serious,” *The National Interest*, March 3rd, Available Online at https://nationalinterest.org/print/blog/buzz/why-india-pakistans-nuclear-rivalry-deadly-serious-129087, Accessed 07-18-2022)

Key Point: If peace ever collapsed, an Indian-Pakistani conflict might not stay regional. Fall out from any nuclear weapons use would devastate the entire world.

While the United States is preoccupied by the threat of nuclear weapons in the hands of potential adversaries such as Russia, China or North Korea, the danger of nuclear conflict may actually be greatest between two of its allies, Pakistan and India. The two nations have engaged in four wars starting since their partition along religious lines in 1947. A fifth could be drastically more costly, as their nuclear capabilities continue to grow and diversify.

Several years ago I made the acquaintance of a Pakistani nuclear science student in China. Curious about the thinking behind his country’s nuclear program, I asked if he really believed there was a possibility that India would invade Pakistan. “There’s still a lot of old-school thinkers in the Congress Party that believe India and Pakistan should be united,” he told me.

I doubt there are many observers outside of Pakistan who believe India is plotting to invade and occupy the Muslim state, but a feeling of existential enmity persists. The third conflict between the two countries in 1971 established India’s superiority in conventional warfare—not unexpectedly, as India has several times Pakistan’s population.

The bone of contention has always been the Indian state of Jammu and Kashmir. At the time of partition, the predominantly Muslim state was politically divided over which nation to join. When Pakistani-allied tribesmen attempted to force the issue, the Hindu maharaja of the region chose to accede to India, leading to the first war between India and Pakistan. Ever since, the line of control between the Indian and Pakistan side has remained bitterly contested, with artillery and sniper fire routinely exchanged. Pakistan intelligence services have infiltrated insurgents and plotted attacks across the border for decades, and Indian security troops have been implicated in human-rights violations and killings of the locals as a result of their counterinsurgency operations.

Pakistan does have to fear the potential of an Indian counterstrike intended to retaliate for a terrorist attack by Pakistani-aligned groups, such as the killing of 166 in Mumbai by Lashkar-e-Taiba in 2008 or the attack on Indian parliament in 2001 by Jaish-e-Muhammad. In both cases, the attackers had ties with Pakistani Inter-Services Intelligence, and Islamabad has shown limited willingness or ability to crack down on these groups. Complicating matters, civilian control of the military is far from consolidated in Pakistan, and it would be quite possible for ISI or some other agency to carry out such activities on its own initiative without the knowledge or support of the head of state.

India’s military has formulated a “Cold Start” doctrine to enable its forward-deployed land forces to launch an armored assault into Pakistani territory on short notice in response to a perceived provocation from Islamabad. This new strategy was devised after the Indian Army’s armored strike corps took three weeks to deploy to the border after the attack on the Indian parliament in 2001, by which time Pakistan had already mobilized its own troops.

Islamabad sees nuclear weapons as its deterrent against a conventional attack, and Cold Start in particular. This is demonstrated by its refusal to adhere to a “No First Use” policy. Pakistan has an extensive plutonium production capacity, and is estimated to possess 130 to 140 warheads, a total that may easily increase to 220 to 250 in a decade, according to a report by the Bulletin of Atomic Scientists.

Many of the new weapons are smaller, short-range tactical weapons intended for targeting frontline troops. To enable a second-strike capability, Pakistan has also empowered local commanders to launch retaliatory nuclear strikes in case the chain of command is disrupted.

While battlefield nuclear weapons are less likely to cause the mass civilian casualties that a strike against a densely populated city would produce, they are deeply worrying in their own way: a state may be more tempted to employ tactical nuclear weapons, and perceive doing so as being intrinsically less risky. However, many simulations of nuclear war suggest that tactical-nuclear-weapon usage rapidly escalates to strategic weapons.

Furthermore, tactical nuclear weapons are necessarily more dispersed, and thus less secure than those stationed in permanent facilities. These issues led the U.S. Army to at first reorganize its tactical nuclear forces in the 1960s, and largely abandon them after the end of the Cold War.

Pakistan fields nearly a dozen different types of missiles to facilitate this strategy, developed with Chinese and North Korean assistance. Ground based tactical systems include the Hatf I, an unguided ground-based rocket with a range of one hundred kilometers, and the Nasr Hatf IX, which can be mounted on mobile quad-launchers. Longer reach is provided by Ghauri II and Shaheen II medium-range ballistic missiles, which can strike targets up to around 1,600 and 2,500 kilometers, respectively.

The Pakistani Air Force’s American-made F-16 fighters are also believed to have been modified to deploy nuclear weapons. The older F-16As and Bs of the Thirty-Eighth Fighter Wing and the newer Cs and Ds of the Thirty-Ninth are both believed to be based near nuclear-weapon storage facilities. The PAF’s five squadrons of Mirage IIIs, based in Karachi and Shorkot, meanwhile, have been modified to launch the domestically-produced Ra’ad nuclear Air-Launched Cruise Missile (ALCM), with a range of 350 kilometers. New JF-17 fighters jointly produced with China are also thought to be capable of carrying the Ra’ad ALCM.

The Pakistani Navy lacks a nuclear strike capability, but appears interested in acquiring one. In January of this year, it released a video claiming to show a test launch of a Babur-3 submarine-launched cruise missile. The domestically produced Babur is similar to the Tomahawk, and designed to approach its target at low altitude to avoid detection. Pakistan already possesses land-based TEL vehicles to deploy the nuclear-capable weapon.

Reflecting its superior conventional abilities, India does adhere to a “No First Use” nuclear weapons policy. Its security posture is also complicated by long lasting tensions with China, dating back to a border war in 1962 in which Beijing seized territory in the Himalayas. Today, China is closely allied economically and militarily with Pakistan, and even has a naval base in Gwadar as part of a strategy to envelop India. India, by contrast, continues to receive much of its weaponry from Russia, but does not enjoy the same kind of military alliance. It has instead dramatically expanded civilian nuclear cooperation with the United States and other nations in the last decades.

India possesses a smaller number of nuclear weapons, estimated in 2015 to range between ninety and 120. However, New Delhi recently acquired a full nuclear triad of air-, land- and sea-based nuclear platforms when it deployed its first home-produced nuclear-powered submarine, the INS Arihant. The Arihant is capable of launching a dozen K-15 Sagarika submarine-launched ballistic missiles. However, these are limited to a range of 750 kilometers, and are thus incapable of reaching the major inland cities of Pakistan or China, a shortcoming India is attempting to address with new K-4 missiles, derived form the land-based Agni-III. New Delhi intends to produce three more nuclear submarines over the years, while Pakistan is considering building one of their own.

India’s chief nuclear arm is thought to lay in its Mirage 2000H and Jaguar fighter-bombers, which can carry nuclear gravity bombs. In 2016, India signed a contract for thirty-six nuclear-capable fourth-generation Rafale fighters from France, further enhancing its aerial striking power. India has also modified its Su-30 fighter-bombers to carry the BrahMos cruise missiles with a range of five hundred kilometers. These could theoretically carry nuclear warheads, though none are believed to have been so equipped so far.

India also has its own array of ground-based nuclear ballistic missiles. The most numerous are slow-firing Prithvi short-range ballistic missiles. Twenty mobile Agni-1 ballistic missiles with a range of seven hundred kilometers are also deployed along the border with Pakistan, while ten heavier Agni-II systems with a range of two thousand kilometers are situated in the northwest for potential strikes on China. India also possesses a small number of rapid-deploying Agni III missiles with a range of 3,500 kilometers, and is developing an Agni IV MRBM and Agni VI ICBM with sufficient range to hit Chinese cities on the Pacific coast.

If there is any silver lining to this steady escalation in nuclear firepower, it’s that neither India nor Pakistan appears to possess chemical or biological weapons. (India completed the destruction of its stock of mustard gas in 2009.) However, the potential for catastrophic loss of human life if nuclear warheads rain down on the cities of the Indian subcontinent is self-evident.

Indian prime minister Narendra Modi and Pakistani prime minister Nawaz Sharif showed goodwill in a surprise meeting in 2015. Unfortunately, neither state appears capable of shaking out of its intractable pattern of conflict, driven by domestic political forces, which makes diplomatic accommodation difficult. The struggle for Kashmir occupies an important part of Pakistani national identity, and there has yet to be a civilian head of state in Islamabad with the will and authority to bring an end to cross-border infiltration and support for terrorist or insurgent fighters. For its part, the Indian Army has failed to respect local Kashmiri leaders and significantly improve its human-rights record.

In 2016 the killing of Kashmiri militant Burhan Wani led to an outbreak of domestic civil unrest in Kashmir that resulted in dozens of civilian deaths. After attackers killed seventeen Indian Army troops in Uri on September 18, the Indian army launched a cross-border raid under murky circumstances ten days later, followed by heavy exchanges of artillery and sniper fire in October and November that killed or injured dozens of civilians and soldiers on both sides of the Line of Control.

The United States sits awkwardly astride the two states. During the Cold War, the United States tilted in favor of Pakistan due to India’s good relations with the Soviet Union. Richard Nixon and Henry Kissinger, against the advice of the State Department, even dispatched a carrier task force in a futile attempt to dissuade India from its support of Bengali independence fighters. However, in recent decades, U.S. diplomacy has moved gradually in favor of democratic India, both due to its potential as a future superpower and its role as a counterbalance to Chinese influence. The role played by President Clinton in helping negotiate the end of the Kargil conflict in 1999 stood as a key turning point in the region—and marked one of the most dangerous confrontations in recent history, as it two nuclear-armed states were at risk of entering into full-scale conflict.

U.S. relations with Pakistan, meanwhile, have worsened despite a continuing flow of American arms for the Pakistani military. This mutual distrust is due to the presence of Islamic militant groups on Pakistani soil and U.S. drone strikes targeting them. Washington and Islamabad have genuinely diverging interests in regards to Afghanistan, the latter desiring to control Afghanistan out of fear that it might otherwise fall under Indian influence. Pakistan, however, can fall back on its relations with China if the U.S. alliance collapses, leading to a complicated diplomatic balancing act.

Despite diverging political agendas on the Indian subcontinent, there should be a common interest in limiting the proliferation of nuclear weapons and the likelihood of nuclear war. Growing arsenals in India and Pakistan serve to increase the catastrophic human cost of a potential conflict between the too, without evidently decreasing the frequency of inflammatory episodes of violence that spike tensions between the nuclear-armed states.

India and Pakistan will of course retain their nuclear arms, and continue to see them as vital deterrents to attack. However, for such policies to remain tenable in the long run, the longtime adversaries must seek to bring an end to a pattern of recurring conflict that is entering its seventh decade this year.

### 2AC — Plan Solves Israel-NATO Cooperation

#### Plan Solves Israel-NATO Cooperation — it cements a process that has already begun.

Bassist 22 — Rina Bassist, Senior Editor at *Al-Monitor*, International Correspondent at *The* *Jerusalem Post*, former Diplomat at the Israeli Ministry of Foreign Affairs, 2022 (“Israel draws closer to NATO,” *Al-Monitor*, June 30th, Available Online at https://www.al-monitor.com/originals/2022/06/israel-draws-closer-nato, Accessed 07-18-2022)

Jerusalem is closely following the annual NATO summit convening this week in Madrid. The dramatic news of an agreement with Turkey for Sweden and Finland to join the alliance has far-reaching implications for the Middle East, Israel and beyond. The new Strategic Concept endorsed yesterday by NATO leaders is also likely to affect its relations with its major non-member partners such as Israel.

Diplomats in Jerusalem and Brussels told Al-Monitor this week that while these geopolitical developments are expected to alter Israel-NATO relations, the changes could actually benefit Israel and make the partnership grow.

Israel realizes that the Russian invasion of Ukraine has undermined the security order in Europe and that the European Union is facing a new era of strategic conflict on the continent. Thus, Europe and NATO are now looking east.

The Russian invasion took place on the backdrop of reforms NATO has been undergoing for the past three years, ever since French President Emmanuel Macron warned that the alliance suffering from "brain death." The Biden administration's commitment to resume its leading role in NATO promises to bring about a healthy process of reforms.

In February 2021, the NATO Secretariat released a proposed road map for a series of reforms. They included addressing emerging technological threats such as cyber and artificial intelligence, preparing the civilian home front for unconventional weapons and confronting the spread of global terrorism.

Another important insight was the understanding that dealing with innovation in the fields of security, production of new strategic tools and confronting technological challenges all require deeper cooperation with the private sector. That means not only collaboration with military industries but also building a dialogue with the software giants and social networks as well as with companies that produce dual-use (civil/military) technologies, all areas of extensive Israeli experience.

For Israel, the developments NATO has been and is undergoing are important for two reasons.

The first is the growing recognition in Jerusalem over the importance of strengthening relations with the alliance. Israeli innovation, its capabilities in the fields of cyber, intelligence, civilian/military interfaces, and the Israeli envelope allowing high-tech to flourish, greatly interest NATO. At the same time, Jerusalem is interested in cooperating with the alliance, which could benefit both its defense systems and the private sector. Israeli companies present at the May Eurosatory 2022 security fair in Paris told Al-Monitor that NATO countries' officials showed great interest in Israeli technologies.

The second is that beyond military and technology cooperation, NATO also serves as a significant diplomatic platform. The alliance offers an arena through which Israel could strengthen its ties with democracies and with Mediterranean countries, including Turkey.

Israel has enjoyed a special relationship with NATO for over three decades and was the third country to gain non-NATO alliance status as early as 1989. Following the Oslo Accords, the organization created the Mediterranean Dialogue Forum to serve as a framework for regional cooperation for peace and to complement other international efforts, such as the Barcelona Process of the European Union and or the Mediterranean Initiative of the Organization for Security and Cooperation in Europe. Along with Algeria, Tunisia, Egypt, Jordan and Morocco, Israel was invited to attend the first meeting of the 1995 Mediterranean Dialogue Forum.

In the following two decades, Israel's relations with NATO focused mainly on the Mediterranean Dialogue. But in the last few years, in parallel with the profound changes within the NATO alliance, Jerusalem has also begun to change direction.

Israel will not abandon the Mediterranean Dialogue, which offers it opportunities for direct encounters with countries with which it does not necessarily have political ties. However, Jerusalem now believes that Israel's value to the alliance (and vice versa) does not lie exclusively on its geographical merits. This period of changes could actually present an opportunity for Israel to integrate into the alliance (from the outside, of course) in a different way. Thus, Israel's geographical importance to NATO has diminished, but Israel's ability to contribute to NATO in terms of intelligence and technology turns the country from a consumer of security to a potential security provider.

Still, with NATO changing, Israel would also need to change. Official Israel, especially the defense establishment, knows how to work well with Israeli defense companies and is accustomed to working with the United States as well as with Germany and the United Kingdom. Trilateral and multilateral cooperation and structured work with external parties such as NATO are not Israeli systems' strong suit.

Nevertheless, it is important to note that Israel has recognized the strategic change that NATO has undergone from the outset and the potential it holds for Israel diplomatically, practically (the defense industries) and strategically in a very broad sense.

The changes in Israel-NATO relations are not only linked to large geopolitical developments and to NATO reforms, but are also highly affected by Israel’s warming ties with Turkey. The deterioration of bilateral relations between Israel and Turkey, especially since the Mavi Marmara flotilla incident in 2010, was also reflected in NATO, with Turkey vetoing Israel's continued participation in military activities of the alliance. Only after Prime Minister Benjamin Netanyahu's 2016 apology was Israel invited to participate in the multilateral military exercise "Black Mountain."

The following year, Turkey agreed that Israel would open an office at NATO headquarters. Israeli diplomats testify that NATO headquarters have become in recent years a significant arena for the transmission of messages between the two capitals.

In his paper for the Israeli Institute for Regional Foreign Policies MITVIM, analyst Roee Kibrik highlights the regional implications and opportunities that warming up relations with Turkey now offers Israel.

The strategic benefit for Israel lies also in expanding the circle of intelligence-sharing. For example, the issue of Iranian terrorism and its emissaries is of great interest to several NATO members. In general, Israel shares intelligence with the Americans and there is also institutionalized cooperation with some major European countries, but Israel shares more limited intelligence with the other NATO members on a regular basis. Expanding the circle means the inclusion of Israeli assessments in the organization's publications, papers that eventually find themselves in the defense ministries of all member states. It's a great way for Israel to highlight strategic issues that are important to it.

In this context, Israel’s Ambassador to the European Union and NATO Haim Regev told Al-Monitor, "For Israel, the NATO alliance is a diplomatic arena for receiving and transmitting messages, but also an important platform to help build the defense establishment's capabilities and reveal diverse Israeli capabilities. The challenges facing NATO and Europe in the wake of the Russian invasion of Ukraine increase the perception of Israel as a significant asset to the alliance and its member states against the background of accumulated knowledge and experience."

Regev added, "Israel's relations with NATO keep growing and deepening in recent years. These relations are based first and foremost on the common democratic values ​​that the alliance represents. Israel is greatly recognized and appreciated for its democratic values and for the experience and knowledge it is willing to share."

Jerusalem estimates that NATO is at the beginning of a process in which the structure of the geographical partnerships transforms into a system based largely on shared values ​​and capabilities. Concerning technologies and security methodologies, say diplomats in Jerusalem, Israel is probably closer to other NATO non-member partners such as Austria, Australia and New Zealand than to North Africa.

### 2AC — Status Quo Solves U.S.-Israel EDT Cooperation

#### Status Quo Solves U.S.-Israel EDT Cooperation — counterplan not needed.

Sarantinos 21 — Argie Sarantinos, Public Affairs Specialist at the U.S. Army Combat Capabilities Development Command, 2021 (“DEVCOM opens office in Israel, fosters partnerships with foreign allies,” DEVCOM Press Release, October 18th, Available Online at https://www.army.mil/article/251266/devcom\_opens\_office\_in\_israel\_fosters\_partnerships\_with\_foreign\_allies, Accessed 07-18-2022)

The Israeli-U.S. technology partnership got a boost recently when DEVCOM stood up its newest International Technology Center, ITC-Mediterranean, in Tel Aviv, Israel. The two-person team is small, but its core mission – to find innovative companies in Israel with cutting-edge technologies – is large.

U.S. Army Combat Capabilities Development Command, or DEVCOM, reaches across international borders to ensure Soldiers have the best technology available by leveraging ITCs strategically located around the world. The ITCs seek opportunities to partner with foreign companies on technologies that support the Army’s key priorities.

“My main goal is to establish DEVCOM, AFC and the U.S. as the research and development partner of choice for the highly innovative technology companies located in this region. We are committed to ensuring U.S. warfighters have access to the world’s best technologies,” said Col. Mike Fleming, ITC-Mediterranean director.

DEVCOM ITCs are located in Europe, Asia, South America, and North America. The ITCs, which are managed by DEVCOM’s three Forward Elements – DEVCOM Americas, DEVCOM Atlantic and DEVCOM Indo-Pacific – are part of the DEVCOM Global Enterprise. The ITC-Mediterranean’s area of responsibility includes Israel, Turkey, South Africa, and United Arab Emirates.

“One of our biggest challenges was establishing relationships with the Israeli Ministry of Defense, the Israeli Defense Force, and the Defense Attaché Office. We also had to become familiar with the technology ecosystem in Israel and learn how to connect DEVCOM with Israel industry partners,” Fleming said.

The ITCs work closely with DEVCOM and the Deputy Assistant Secretary of the Army for Defense Exports and Cooperation on the Army’s Engineer and Scientist Exchange Program, or ESEP, which pairs DOD civilian scientists and engineers with embedded positions in partner nations. The yearlong assignment creates opportunities to work collaboratively using laboratories, personnel, facilities, equipment, and other partner technology resources that support the Army’s modernization priorities.

“While we continuously look for new ways to partner with industry, we also identify research grant and cooperative agreement opportunities with international scientists and across the Army research enterprise. These partnerships form the basis of the Basic & Applied Research mission,” said James Mullis, ITC-Mediterranean technical director.

In addition to scouting for foreign technology, the ITC’s facilitate the international armaments cooperation mission by providing boots on the ground to meet fact-to-face with leadership of partner nations. The ITCs connect personnel from these nations with U.S. researchers and technical project officers and facilitate sharing research, development, and test and evaluation information on defense technologies, systems, and equipment using data exchanges agreements. Their mission also includes supporting cooperative projects and procuring foreign technology and equipment and logistics.

Collaborating with international partners is a critical part of the DEVCOM Global Enterprise mission, and the ITC-Mediterranean office is a key part of this effort. These partnerships will ultimately play a role in providing the best technology available to Soldiers.

### 2AC — Plan Solves India-NATO Cooperation

#### Plan Solves India-NATO Cooperation — they’re amenable to an expanded relationship.

Mohan 22 — C. Raja Mohan, Visiting Research Professor at the Institute of South Asian Studies—an autonomous research institute at the National University of Singapore, Senior Fellow at the Asia Society Policy Institute (India), former Professor of South Asian Studies at Jawaharlal Nehru University (India) and at the S Rajaratnam School of International Studies at Nanyang Technological University (Singapore), holds a Ph.D. in International Relations from Jawaharlal Nehru University (India), 2022 (“India’s NATO Engagement: Old Inhibitions and New Imperatives,” Institute of South Asian Studies Brief, July 12th, Available Online at https://www.isas.nus.edu.sg/papers/indias-nato-engagement-old-inhibitions-and-new-imperatives/, Accessed 07-18-2022)

Traditionally, India has been stone-cold in its responses to the offers of engagement from the world’s most powerful military alliance – the North Atlantic Treaty Organization (NATO). India’s reluctance is rooted in its traditional policy of non-alignment and its enduring strategic partnership with the Soviet Union and later Russia.

India’s stand-off attitude, however, faces a new context that at once limits the possibility for New Delhi’s engagement with the alliance and generates new imperatives to engage NATO.

The negative side of the ledger is the deepening conflict between Russia and NATO after Moscow’s aggression against Ukraine. As New Delhi carefully navigates the complex dynamics between Russia and NATO, India is unlikely to make a radical departure in its thinking. India’s earlier signals of a softening attitude towards NATO might be harder to pursue amidst the war in Europe today.

New Delhi had, in fact, invited NATO’s Secretary-General Jens Stoltenberg to speak at the Indian Foreign Office’s premier international forum – the Raisina Dialogue – in April 2021. This was the first time the NATO leadership had participated in an official Indian forum.

During his address, Stoltenberg affirmed that “India was at the forefront” of many shared security challenges, including “Afghanistan, international terrorism, to maritime security”. He insisted that there was more that India and NATO “can do together”, including “consult, coordinate and take concerted action”.

Meanwhile, the ideological questions about non-alignment are becoming less meaningful in the prospects for engagement between India and NATO. India today is closer than ever before to the Western world. New Delhi has a strong strategic partnership with key Western countries, including the United States (US) and France. India has also stepped up security dialogue with the European Union.

India has also shed some of its opposition to plurilateral arrangements with the West. It is now an active member of the Quadrilateral Security Dialogue (also called the Quad) that brings India together with Australia, Japan and the US. However, India has carefully avoided branding the Quad as a military alliance, as some of its activities have a significant strategic and security orientation. India also conducts the ever more sophisticated annual Malabar naval exercises with the US and its Asian allies – Australia and Japan.

Meanwhile, Russia’s invasion of Ukraine has pushed two neutral states of Europe – Sweden and Finland – into seeking NATO membership. In the early decades of the Cold War, Sweden was an important partner of India in developing collaboration between neutral and non-aligned states. No ideology can be immune from changing circumstances. India’s ideology of non-alignment and opposition to military blocs has been steadily modified in its post-Cold War international relations.

India actively participates in the Shanghai Cooperation Organisation (SCO), led by Russia and China, which has many military dimensions. India is an active member of the SCO, which is designed to limit US influence in inner Asia, but it is reluctant to engage NATO, underlining the real but unstated pro-Russian bias in Indian security policy. It has little to do with the ideology of non-alignment but everything to do with the special relationship that New Delhi has built with Moscow over the last few decades.

However, India’s Russian partnership is increasingly constrained by Moscow’s growing tensions with the West as well as its deepening strategic partnership with China. This coincides with the steady deterioration of India’s ties with China and the sharpening conflict between Washington and Beijing.

As balancing China becomes the dominant imperative for India, it has embraced the idea of the Indo-Pacific, helped revive the Quad, and welcomed the growing interest of the European powers, including France, the United Kingdom and the EU, in the region.

Although India has not formally welcomed NATO’s growing outreach to the Indo-Pacific in recent years, it has no ostensible reason to quarrel with it either. Any additional pressure on China from Europe and NATO cannot but serve India’s interest in balancing Beijing. After all, in the last few years, India has often tried to persuade Russia to tone down its hostility toward the Indo-Pacific, if with little success.

What we have seen is a tightening embrace of Russia and China that complicates India’s regional calculus. Moscow and Beijing have drawn closer, especially after they unveiled a partnership “without limits” and no “forbidden areas” just days before Moscow’s invasion of Ukraine in February 2022.

This, in turn, has intensified a drift towards the integration of the Asian and European theatres, which were long seen as separate. The circle was closed at NATO’s Madrid summit in June 2022, which saw the first ever participation of the prime ministers of Australia, Japan and New Zealand and the president of South Korea.

As the new interactive dynamic between the Sino-Russian strategic partnership and NATO’s Asian engagement unfolds, India cannot forever take a segmented approach to Europe (and Russia) on the one hand and the Indo-Pacific (China) on the other. As New Delhi recalibrates its strategy, engagement with NATO must inevitably figure in India’s geopolitical agenda.

Beyond the question of India adjusting to the shifting geopolitical terrain, there are significant immediate benefits for New Delhi in any bilateral engagement with NATO. As a former senior US official, A Wess Mitchell, put it, India can gain substantially from a partnership with NATO, including military, strategic and technological, without in any way constraining its broader strategic options.

Sceptics will keep their fingers crossed. However, optimists will point out that India has made many unprecedented changes to its international relations in recent years – if quietly and in an incremental manner. It will be no surprise then if India’s attitude to NATO will continue to evolve in the coming years.

## AT: Unilateral/Domestic CP

### 2AC — DOD Procurement Process Reform Fails

#### DOD Procurement Process Reform Fails — only the plan sets strategic EDT priorities that accelerate tech procurement.

Sisson 22 — Melanie W. Sisson, Fellow in the Center for Security, Strategy, and Technology at the Brookings Institution, former Vice President of Analysis at Govini—an early-stage national security artificial intelligence and machine learning technology company, former Senior Fellow and the Director of the Defense Strategy and Planning Program at the Stimson Center, hold a Ph.D. in Political Science from the University of Colorado-Boulder, 2022 (“Why can’t the Pentagon buy the cutting-edge technology it needs?,” *Tech Stream*—a Brookings Institution blog, February 23rd, Available Online at https://www.brookings.edu/techstream/why-cant-the-pentagon-buy-the-cutting-edge-technology-it-needs/, Accessed 07-15-2022)

Silicon Valley’s frustration with the Department of Defense is both well-known and well-founded. All too often, the department provides initial funding to develop a promising technology, only to fail to deliver funding adequate to sustain a scaled capability. This gap between initial and sustained funding is so well-known that it has nickname—the so-called “valley of death”—and it makes the Pentagon an unreliable partner. It has gotten bad enough that when defense and technology officials recently convened for the annual Reagan National Defense Forum in California, investors and technologists made clear that their collective tolerance for the Pentagon’s inability to work effectively with the defense innovation base is nearing the point of no return.

The Defense Department is aware of this criticism and has sought to address it via meaningful reform. In a report from earlier this month on competition in the defense industrial base, the DoD reports that these efforts have achieved creditable success in increasing engagement with small businesses through the use of tools like the “Other Transaction Authority,” the “Small Business Innovation Research,” and the “Small Business Technology Transfer” programs. The 2022 National Defense Authorization Act (NDAA) includes similar reform provisions instructing the DoD to streamline contracting—especially of systems that enable software development and adoption—and to expand engagement with new and underused vendors. It also includes an important provision establishing a committee to review and to make recommendations about how to best revise the Planning, Programming, Budgeting & Execution Process (PPBE), the means through which the Pentagon allocates its resources.

These measures are sensible but should not be expected to solve the DoD’s difficulties acquiring the technology it needs to build a modernized military. Process change can reduce barriers to acquisition, but it will not remove the central impediment: The problem isn’t that the DoD doesn’t know how to buy; it is that it doesn’t know what to buy.

Function-first acquisition

The DoD’s approach to technology has its origins in the Cold War. In the 1950s, President Dwight Eisenhower faced the difficult problem of how to counter the Soviet Union’s much larger conventional forces without devoting the entirety of the federal budget to defense spending. The solution was the concept of “offset,” the idea that the United States could find a way to compensate for its disadvantage in the relative balance of forces in Europe. Eisenhower’s approach to offset, the “New Look” strategy, relied upon surpassing the Soviets in the emergent technologies of the day—nuclear weapons and the airplanes and missiles to deliver them. This would balance out the Soviet Union’s conventional advantage, and at manageable expense to the U.S. taxpayer.

This first offset strategy lasted only as long as it took the Soviet Union to achieve nuclear parity, and by the early 1970s the United States once again needed a means of compensating for the Soviet advantage in conventional assets. The second attempt at offset focused not on increasing the kinetic power of individual munitions nor on amassing the platforms to deliver them, but on ensuring that targets could be reliably hit. The result was a revolution in precision warfare, generated by investments in guided munitions and in the radar, positioning, and communications networks upon which they rely.

In the 1990s, the second offset and the collapse of the Soviet Union left the United States with a large arsenal more capable than ever before of locating and destroying adversary hardware at distance and an environment in which there was little pressure to evolve operational concepts. If anything, the 1991 Gulf War and the air war in Kosovo seemed to affirm existing concepts, and the long, consuming counterinsurgency campaigns in Afghanistan and Iraq in the 2000s demanded use of current capabilities more than the development of new ones. The Department of Defense thus was under little pressure to think about technology as anything other than the constituent parts of large platforms and systems designed to deliver kinetic force—a paradigm that led to the procurement of the functionally dubious F-35 Lighting II Joint Strike Fighter program in 2001 and the similarly troubled Gerald R. Ford class of nuclear-powered aircraft carriers in 2008.

By 2014, however, a group of senior defense officials convinced that growth in China’s military capabilities was putting U.S. interests in the Indo-Pacific at risk revived the idea of offset. This time, the idea was that the United States could offset China’s geographic advantage by using modern technologies to enable the U.S. military to “project power and to dominate force-on-force encounters.” The thinking behind the third offset influenced the 2018 National Defense Strategy and energized the Pentagon’s interest in modernization. It did not, however, break the habit of defining modernization in terms of large, technology-laden platforms capable of carrying out precision strikes from distance. This fixation persists despite compelling analysis that now should temper claims about the success of this type of high-tech warfare in Kosovo and Iraq (both times).

Initial victories in these conflicts tempted many analysts to conclude that technological prowess had given the United States a decisive advantage. After-action assessments deflate these conclusions. In Kosovo, the success of the air campaign was measured primarily in terms of U.S. and NATO losses—outcomes determined more by rules of engagement than by the technology used. In Iraq, assessing the impact of precision-guided munitions at the outset of both invasions is complicated by the fact that they often were used in conjunction with less sophisticated, unguided ordnance. Nonetheless, enough data are available for serious analysts of both wars to highlight the importance of so-called “legacy” assets in completing critical tasks and to stress that the capabilities of the adversary, the terrain, and even the weather were particularly conducive to U.S. operations.

None of these conditions would be met in a conflict with China. China’s electromagnetic, air, cyber, and missile capabilities are formidable; its surrounding seas and coastal terrain are not static, flat, and featureless; and the PLA is well-trained and committed. These characteristics reduce the value of large, centralizing platforms—like aircraft carriers and the planned Joint all Domain Command and Control (JADC2) system—and increase the return on investment in technologies that promote flexibility, support mobility, and enable localized decisionmaking.

The Marine Corps offers an example of what this kind of technology pragmatism looks like. The Commandant’s Planning Guidance from 2019, the Force Design 2030 from 2020, and A Concept for Stand-in Forces from last year together offer a cohesive, if still developing, description of what the Marine Corps must be able to achieve in the near term and of how to do so. Clarity about the functions the Marine Corps must fulfill begets clarity about the role of technology, and so it is pursuing mobile, expendable tools that enable small and dispersed elements to conduct reconnaissance and to make timely, informed choices about maneuver and engagement. These capabilities will be useful in a high-end warfight, should that be necessary, and also in the conduct of daily competition—used to detect unwanted adversarial behaviors short of war and to mobilize to deter or rebuff them quickly. When faced with the option of continuing to chase future funding for a next-generation multifunctional drone system or to purchase the proven MQ-9 Reaper this year, the Marines chose the latter, a decision that prioritized function over form. The 2022 NDAA-mandated commission to review the PPB&E process might take note of this as a demonstration of how coherent strategy makes it possible to reconcile the tension between short-term budgeting and long-term force planning.

Informed buyer

Technology firms often credit individual leadership with acquisition successes. When there is a buyer who understands how a tool will be useful, the DoD process is a hurdle, but not an obstacle, on the way to getting a deal done. This does not require expertise in technology. Knowing how a technology works is not prerequisite to understanding how it can be used. Knowing what needs to be done, however, is prerequisite to understanding whether a technology will be useful.

Today’s technology companies are especially good at designing tools to fulfill clearly articulated functional needs. The areas in which the greatest advances are being made are in capturing data and in using sophisticated processing techniques—like machine learning—to enable people to make more informed choices, faster. The imperative for the Services and Joint Staff therefore is not to seek grand system-of-system solutions, but rather to identify common and recurrent operational tasks for which the addition of information, or of more timely information, will help forces know where to be, what to expect when they get there, and how to maximize their likelihood of mission success. For the defense-wide organizations, the imperative is to identify business questions that currently go unanswered, to find ways to reduce transaction costs, to enhance productivity, and generally to make the experience of working for the DoD better.

The DoD acquisition process is an easy target for Silicon Valley’s ire. Yet it is far from clear that process reform alone will make the DoD a better buyer. It is not wrong, after all, for the process to demand that fiduciaries of public money articulate functional goals, define achievable requirements, set feasible milestones, fund at realistic levels, and be held accountable to those plans. But in the absence of pragmatic, clearly defined strategies to drive acquisition, process reform on its own will never deliver the modernized military that the United States needs.

### 2AC — Domestic Innovation Reform Fails

#### Domestic Innovation Reform Fails — only the plan solves by re-booting the U.S. innovation ecosystem.

Darby and Sewall 21 — Christopher Darby, Chief Executive Officer at In-Q-Tel—a not-for-profit investment firm working on behalf of the U.S. national security community, former Vice President and General Manager at Intel, and Sarah Sewall, Executive Vice President for Policy at In-Q-Tel, former U.S. Undersecretary of State for Civilian Security, Democracy, and Human Rights, 2021 (“The Innovation Wars: America’s Eroding Technological Advantage,” *Foreign Affairs*, March/April, Available Online at https://www.foreignaffairs.com/articles/united-states/2021-02-10/technology-innovation-wars, Accessed 07-15-2022)

A Market Mindset

Supporting those priorities is another matter altogether. The current approach—with the government funding only limited research and the private sector taking care of commercializing the results—isn’t working. Too much government-funded research remains locked in the lab, unable to make the leap to commercial viability. Worse, when it manages to leave U.S. government labs, it often ends up in foreign hands, depriving the United States of taxpayer-financed intellectual property.

The U.S. government will need to take a more active role in helping research make it to the market. Many universities have created offices that focus on commercializing academic research, but most federal research institutions have not. That must change. In the same spirit, the U.S. government should develop so-called sandboxes—public-private research facilities where industry, the academy, and the government can work together. In 2014, Congress did just that when it established Manufacturing USA, a network of facilities that conduct research into advanced manufacturing technologies. A similar initiative for microelectronics has been proposed, and there is no reason not to create additional sandboxes in other areas, too.

The U.S. government could also help with commercialization by building national data sets for research purposes, along with improved privacy protections to reassure the people whose information ends up in them. Such data sets would be particularly useful in accelerating progress in the field of artificial intelligence, which feeds off massive quantities of data—something that only the government and a handful of big technology companies currently possess. Success in synthetic biology, along with wider medical research, will also depend on data. Thus, the U.S. government should increase the quantity and diversity of the data in the National Institutes of Health’s genome library and curate and label that information so that it can be used more easily.

All this help with commercialization will be for naught, however, if the startups with the most promising technologies for national security cannot attract enough capital. Some of them run into difficulties at the early and late stages of growth: in the beginning, they have a hard time courting investors willing to make high-risk bets, and later on, when they are ready to expand, they find it difficult to attract investors willing to write large checks. To fill the gaps at both stages, the U.S. government needs its own investment vehicles.

We work at the parent company of In-Q-Tel, which offers a promising model for early-stage investment. Created in 1999 by the CIA, In-Q-Tel is an independent, not-for-profit firm that invests in technology startups that serve the national interest. (One early recipient of In-Q-Tel’s investment was Keyhole, which became the platform for Google Earth.) Now also funded by the Department of Homeland Security, the Department of Defense, and other U.S. agencies, In-Q-Tel identifies and adapts innovative technologies for its government customers. Compared with a federal agency, a private, not-for-profit firm can more easily attract the investment and technology talent required to make informed investments. There is every reason to take this model and apply it to broader priorities. Even just $100 million to $500 million of early-stage funding per year—a drop in the bucket of the federal budget—could help fill the gap between what the private sector is providing and what the nation needs.

For the later stage, policymakers could draw inspiration from the U.S. International Development Finance Corporation, the federal agency responsible for investing in development projects abroad, which in 2018 was first authorized to make equity investments. A late-stage investment fund could be structured as an arm of that agency or as a fully independent, not-for-profit private entity funded by the government. Either way, it would provide badly needed capital to companies ready to scale up their operations. Compared with early-stage government support, late-stage government support would have to be greater, in the range of $1 billion to $5 billion annually. To expand the impact of this government investment, both the early- and the late-stage funds should encourage “sidecar” investments, which would allow profit-seeking firms and individuals to join the government in making, and potentially profiting from, technology bets.

Government-sponsored investment funds like these would not only fill critical gaps in private-sector investment; they would also allow taxpayers to share in the success of research their money has funded. Currently, most government funding for technology comes in the form of grants, such as the Small Business Innovation Research grants administered by the Small Business Administration; this is true even of some programs that are billed as investment funds. This means that taxpayers foot the bill for failures but cannot share in the success if a company makes it big. As the economist Mariana Mazzucato has pointed out in these pages, “governments have socialized risks but privatized rewards.”

Not-for-profit investment vehicles working on behalf of the government would have another benefit: they would allow the United States to play offense when it comes to technological competition. For too long, it has played defense. For example, it has banned the export of sensitive technology and restricted foreign investment that might pose a national security risk—even though these actions can harm U.S. businesses and do nothing to promote innovation. Supporting commercialization with government-sponsored equity investment will not be cheap, but some of the upfront costs would likely be regained and could be reinvested. There are also nonmonetary returns: investing in national priorities, including infrastructure that could be exported to U.S. allies, would enhance the United States’ soft power.

Innovation Ever After

President Joe Biden has pledged to “build back better” and restore the United States’ global leadership. On the campaign trial, he laid out promising proposals to promote American innovation. He called for dramatically boosting federal R & D spending, including some $300 billion to be focused on breakthrough technologies to enhance U.S. competitiveness. That is a good start, but he could make this drive far more effective if he first created a rigorous process for identifying top technological priorities. Biden said he supports “a scaled-up version” of the Small Business Innovation Research grants and has backed “infrastructure for educational institutions and partners to expand research.” Even greater opportunity lies in filling the gaps in private-sector investment and undertaking a long-overdue expansion of government support for commercialization.

On innovation, if the United States opts for just more of the same, its economy, its security, and its citizens’ well-being will all suffer. The United States will thus further the end of its global leadership and the unfettered rise of China. Biden has the right instincts. Yet in order to sustain its technological dominance, the country will have to fundamentally reenvision the why and how of innovation. Biden will no doubt be consumed with addressing domestic challenges, but he has spent much of his career promoting the United States’ global leadership. By revamping American technological innovation, he could do both.

### 1AR — Domestic Innovation Reform Fails

#### Allied integration is the only way for the U.S. to win the tech race — the Cold War proves.

Farley 21 — Robert Farley, Senior Lecturer in the Patterson School of Diplomacy and International Commerce at the University of Kentucky, former Faculty Member in the Department of National Security Strategy at the U.S. Army War College, holds a Ph.D. in Political Science from the University of Washington, 2021 (“Innovation Offense vs. Defense,” *The Diplomat*, July 24th, Available Online at https://thediplomat.com/2021/07/innovation-offense-vs-defense, Accessed 07-18-2022)

Washington is awash in proposals to enhance technological innovation, while at the same time limiting the extent to which that innovation spreads to competitors like Russia and China. As the United States cannot rely on massive economic advantage over its adversaries (China, anyway), technological innovation appears to be the way to maintain U.S. military advantages worldwide. In this context, does it make more sense to focus on offense (enhanced innovation) or defense (protecting that innovation from snoopers)?

Many of the proposals for enhanced innovation, whether in legislation or in think tank projects, have a few things in common. They involve developing human capital to pursue high-tech fields, making it easier for government to consistently access high technology, improving government funding for primary and applied research, and laying the infrastructural foundations for further research and development. On the defensive side, they envision better cybersecurity, tighter export controls on advanced technologies, and better monitoring of foreign investment in the technology sector.

None of these are bad things, per se. It cannot be overstated, however, that the question of military technological supremacy is intimately tied both to overall economic performance and to global economic integration. The United States won the technological race in the Cold War in large part because it created and then could rely upon a global network of trade and innovation. China’s export-driven economy has benefited immensely, from a technological point of view, from its integration into global supply chains.

This is another way of saying that the technological aspect of U.S.-China competition will not focus fundamentally on the appropriation or theft of particular kinds of military technology. That was certainly an aspect of the Cold War, in large part because the technological preconditions of the U.S. and the USSR were so radically different. Defensive measures should not be ignored, but enhancing the productivity of the defense industrial base will bring higher dividends than protecting its products. Rather, both Beijing and Washington need to focus on creating the preconditions of consistent military technological innovation, remaining attentive to but not paranoid about what the other side is doing.

It seems likely that technological competition will not play out in terms of a single sharp break, with the jagged edges then protected by walls of export controls and travel restrictions. The political, social, and economic logics of China-U.S. trade relations are too deeply twined together to allow a relationship similar to that which held between the U.S. and the USSR in the 1950s and 1960s. The best defense, it seems, will be to lay the foundations of a healthy, productive, and innovative defense industrial base.