# Aff---AI Logistics---Starter Pack

## 1AC

### Advantage One---NATO

#### Artificial Intelligence is on the brink of transforming warfare---NATO is developing a governance strategy now but testing is key to effective implementation---it demonstrates value in real-time to ensure buy-in, evolves models to optimize decision-making, and resolves the skills gap

George Christou 21, Professor of European Politics and Security, University of Warwick. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

Just like with the commercial and public sector, then, technological progress has allowed militaries and security sector professionals to gather large amounts of data, and a number of countries (governments and armed forces) are in the process of constructing and implementing governance models to ensure the benefits of Big Data in terms of real time intelligence, enhanced decision-making, situational awareness and overall competitive edge against increasingly capable opponents. The synergy between Big Data, ML and AI is particularly important in this context when it comes to all aspects of combat readiness, with experts agreeing that AI and its application in the armed forces is “present in all domains…and all levels of warfare” (Svenmarck et al., 2018) with the potential to have a transformative impact on national security technology (Allen and Chan, 2017; see also Tonin, 2019). Many, however, are at an early stage in the development of any BDA strategy. Thus, the lessons from other sectors – and indeed leading governments and security organizations – can provide guidance on best practice as they move from their ‘data’ governance models to ‘Big Data’ governance frameworks that will give them the ability to ensure maximum value and advantage is extrapolated from the BDA life-cycle.

The first lesson or best practice relates to having a clear rationale, goals and guiding principles in place to ensure effective governance of Big Data in the organization. This includes strategically assessing the type of model required, based on current capabilities, resources and future needs, i.e. decentralized/centralized/hybrid. More importantly, governments and security organizations need a clear understanding of the value of Big Data across different domains (land, sea, air) and landscapes (human, physical, information) so that high quality, usable, real-time information can be delivered through AI and ML at strategic, tactical and operational levels. This is certainly recognized in the NATO context, with a Dutch Position Paper highlighting that, in terms of Big Data and AI, “the focus should be on assessing and…demonstrating the added value that innovations can provide to NATO military theatres” (Smallgange et al., 2018). This is critical, so that the full possibilities of influencing the three landscapes – through situational awareness and effective command and control – can be developed in a broader way than that offered by traditional military means. This way, there is also a recognition that in order to take full advantage of the data-centric technologies (BDA and AI), a data-centric methodology is required, so that effective support can be offered at different levels (Blunt et al., 2018).

In the second place, related to the first lesson learned, in a military and security context where there is often a unified command in combination with tiered formal hierarchy that tends towards specialization, there can also be structural inefficiencies in the flow of information; operating jointly can thus often come at a high cost (Zelaya and Keeley, 2020). When considering any data-driven methodology, then, much thought has to be given to the organizational data management life cycle – including how to integrate the use of BDA and new technologies (e.g. AI, ML) with human decision-making, control and communication of information. Indeed, it has been argued that whilst BDA and associated technologies offer significant advances in rapidly collecting, processing and deciphering complex forms and varieties of data for the purposes of action, the human element is still critical in contextualizing any such data and offering insights on the complexity and “shades of grey” that might be missed by BDA (Van Puyvelde et al., 2018: 1414; see also Desclaux, 2018: 9). To this end, thought has already been given to the implementation of the Observe, Orient, Decide, Act (OODA) loop to determine the type of decision support required and how meaningful human control can be enabled. The OODA perspective or approach, it is argued, represents “the life cycle from data acquisition to decision making and also reflects how sophisticated a technology should be in order to provide value” (Smallgange et al., 2017: 6). An important element within this loop is giving full consideration to any legal, ethical and moral questions that arise in relation to action and particularly the use of lethal autonomous weapon systems (LAWS).

The third best practice relates to buy-in from the organization as a whole. That means not just having the technology, tools and mechanisms in place within a data driven environment that ensures access to and use of Big Data for all team members, but also: a) Leadership from those at the top (Commanders) and within the different echelons of command within and across domains, landscapes and levels through to data engineers, analysts, assessors, translators – and the ability of the various communities of interest to use data communicated to them in an effective way; b) The creation of an organizational (big) data-driven culture and data-centric paradigm – including ensuring that all relevant staff are data literate, have the requisite skills, literacy and readiness, and are provided with the education, training and skills to operate effectively. To this end, NATO has identified a key capability gap when it comes to literacy and readiness and has also recognized that in terms of recruiting AI specialists, engineers and data scientists the pool of talent is shallow and it can be difficult to compete with Big Tech companies.

Here, leading national governments in developing their Big Data strategies have sought to ensure the requisite investment is in place going forward for developing a (resilient, secure and trusted) technology architecture and recruiting the right talent. They have also, alongside leading security organizations such as NATO, recognized that partnerships (in particular with industry) and contracted services, as well as in-house expertise, that will be needed to deliver and sustain the necessary skills and understanding for assessing, interpreting and communicating information in an effective way (Tonin, 2019; Blunt, 2018; Defence IQ, 2020; Big Data for Defence, 2019). Finally, the non-defense commercial/industry sector will not just be important in terms of the skills and expertise element, but also for technological adaptation and integration, given that many innovations stem from commercial companies; the UK government, for example, has awarded IBM a GBP 3.8 million deal for the development of an AI-powered military software platform prototype (Defence IQ, 2020). More broadly, governments and security sector organizations will have to overcome certain hurdles – organizational, cultural, and incentive structures – to ensure that new technologies are adapted so they can bring advantages across strategic, tactical and operational levels (Kostopoulos, 2019: 9) and allow efficient and effective decision-making when needed.

Conclusions This chapter has highlighted the central ways in which commercial organizations have been successful in constructing and executing a BDA strategy, and discussed the main pitfalls that organizations should seek to avoid in embarking on any such strategy. In this context it is clear that there are many lessons to be learnt and best practices that can be adapted by the security sector in relation the integration of BDA into existing strategies. Indeed, a cursory look at the leading nations with regards to Big Data strategies – and security organizations such as NATO – demonstrate that their central objectives have been developed (and appropriately adapted) with commercial best practice in mind in relation to data management, governance and analytics.

To this end, there are general principles for success that are underpinned by a need for a clear rationale, goals and strategy, a strong leadership, an agile, resilient, secure and adaptable technical infrastructure, a data-centric approach and methodology, and a data culture that permeates the whole organization. Of course, this chapter did not have the space or scope to discuss the micro-level BDA requirements within the security sector in relation to all dimensions, and in particular innovative hardware and software architectures or indeed process techniques and challenges.

What is clear going forward, however, is that the security sector will face challenges of a technical and nontechnical nature that will require financial investments in AI systems and human talent, as well as cooperation and collaboration with industry and leadership, if BDA strategies are to deliver the advantages expected to those engaged at strategic, tactical and operational levels. In this, lead nations and organizations, whilst not starting from scratch, have clearly started to negotiate the steep learning curve when it comes to Big Data and decision-making (Street et al., 2019). They are at a formative phase of development with regards to constructing and implementing strategies and governance frameworks, and indeed modelling and simulation environments, tools and techniques to allow them to derive maximum value from Big Data. The journey ahead, however, whilst entailing certain risks, is also an opportunity – if objectives and goals are clearly defined, strategies grown and adapted according to ever-changing needs, data and technological environments, and data governance and management practices enabled by strong leadership are underpinned by a philosophy of date-centric methodology, technology and clear legal and ethical code of conduct. Testing (through exercises, simulations, etc.), failure and the ability to reflect are important components of evolving and (re)defining BDA governance so that real value can be extracted in real time, with trustworthy and accurate data, and systems, technology and skills required to exploit data all the way through the decision-making process are sustained.

#### NATO AI governance solves hybrid tactics, run-away offensive cyber weapons, great power conflict, and internet functionality---diffusion of tech is inevitable but cooperation through NATO is key to standardization that leads to effective management

Sonia Lucarelli et al 21. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

Digital revolution has substantially transformed the world we live in, providing great opportunities but also making societies more vulnerable and transforming the meaning of state borders. Technology makes external interferences cheaper, faster and all-encompassing: citizens can potentially become direct targets of information warfare, all members of a society can be part of conflicts one way or another. From advanced weaponry to command and control, most security-related domains are undergoing deep transformations as data availability and transmission increase exponentially. This is especially true as the emergence of so-called hybrid tactics contributes to universalize the battlefield. Also, attackers may lose control of their offensive cyber weapons, and ‘collateral damages’ across the private sector and the public worldwide might be more and more difficult to contain. Less visible, yet important challenges connected with Information Communication Technologies (ICTs) also exist. For instance, data overload can create problems for decisionmakers that are unable to detect important signals. Losing sight of how machines make their calculations – a somewhat inherent feature of Artificial Intelligence (AI) – can hinder deeper understanding of phenomena as well as learning, besides having dense ethical implications.

A crucial question for Western societies and governments is how to deal with technological changes by exploiting their many benefits while managing to limit their risks. Broadly speaking, observers have long noticed the potentialities of technologies in the security domain: better situational awareness, early warning against threats and risks, the ability to prevent and/or stop attacks to happen, the use of technology against the adversaries’ own technologies, and eventually deterrence of high-end hybrid warfare or, at least, the increase of resilience against it. In particular, in order to harness the potential of new technologies, higher levels of security are needed. While internet is unfortunately not secure by design, it has to be somehow retrofit to guarantee a certain level of protection – for instance by avoiding a single point of failure, developing better firewalls, etc. Ultimately, the digital revolution poses challenges to decision makers both as potential users of new technologies and as leaders of targeted societies. Learning to achieve political aims through the support of technological innovations and at the same time acquiring the ability to prevent and manage interferences, if not attacks, have become paramount.

However, achieving such results is not only about engineering. Technologies need ad hoc governance, organizations and skilled users to properly function. Actually, history is full of examples of good technologies that were improperly used and/or unable to provide the expected gains. Therefore, a joint, multi-disciplinary efforts is needed to think and manage technologies in a more comprehensive and secure way across various domains. For instance, the very same design of AI needs exchanges with social scientists in order to limit analytical biases and increase the quality of data that will then be processed through Machine Learning (ML). Moreover, many public policies involve technologies with a strong security dimension. This is one of the main reasons security standards should be harmonized across individual government’s policies as well as among Allies: this is what has been leading NATO’s renewed efforts on standardization beyond the strictly military perimeter, for instance towards the 5G domain.

While digital technologies continue to dramatically increase in scope and relevance, they are deeply embedded into the broader geopolitical framework, with the re-emergence of multipolarism and looming great power confrontation. This connection has to be discussed and understood as it affects not only security but also economic and technological domains. The globalized supply chain of technology building block entails vulnerabilities and dependencies on unreliable suppliers. Foreign Direct Investments (FDIs) in hightech companies, Small and Medium Enterprises (SMEs) and critical infrastructures are guided not only by an economic rationale but also by a politico-military one, and have to be monitored accordingly. Cyber space and, partly, outer space are de facto unregulated global commons where the ability to set regulations and standards could be a matter of competition and/or cooperation among major countries worldwide. The notions of ‘whole-of-government’ and ‘whole-of-society’ approaches confirm that these problems should be dealt with comprehensive strategies.

Great and middle powers increasingly rely on stand-off weapons, both physical and cyber ones, able to create damages rapidly, worldwide and on a large scale. This trend is going to be accelerated by AI. Some countries are adopting principles on responsible use of AI, including in terms of control and accountability. However, a vacuum remains in international law. And such vacuum is more difficult to fill because of the aforementioned interaction between geopolitics and technologies. Different powers conceive technology – and what it can bring them in terms of benefits – in different ways, and they are unwilling to regulate internationally this field of competition and warfare.

In such a rapidly changing security environment, NATO and allied activities directly or indirectly defend citizens’ daily life. In the age of Big Data, AI and the pervasive use of internet, the challenge is to defend the ever-expanding information environment while maintaining all its functionalities.

Against this backdrop, in the post-Cold War period NATO somehow missed the opportunity to involve Allies and partners in a debate on how defense technologies and norms have been changing with the ICT revolution. The result is that the web is not secure by design, and both private and public actors struggle to mitigate risks and threats in an unregulated environment where attackers are structurally advantaged over defenders. Today, the Alliance should not miss the opportunity twice vis-à-vis Big Data, AI and, broadly speaking, the current and future (r)evolution of ICT. The aim of the 2020 Academic Conference was precisely to explore some fundamental aspects of the challenges and opportunities posed by technological change to the security environment in which NATO works. Below follows a brief introduction to NATO, cyber defense and three sets of issues investigated in closer detail: Big Data and decision-making; hybrid threats to allied decision-making; AI adoption by allied armed forces.

NATO, Cyber Defense and Emerging Disruptive Technologies NATO begun to focus on cyber defense already in 2008, and over time it built up institutions and frameworks to deal with it from a well-limited military perspective. Allies recognized a cyber attack could lead to the activation of Article 5 of the Washington Treaty on collective defense. In that case, there is a clear procedure where NATO authorities take the military lead. Article 5 does not prescribe a clear procedure factoring in new technologies. On a regular basis, headquarters and the Secretary General cabinet carry on exercises on situational awareness, whereby they receive intelligence and military advice and are immersed in an information space with blue and red teams. Moreover, every two years, there is a large-scale exercise involving national governments. These efforts aim to build familiarity with the technology-related security challenges. However, further evolution of AI-based cyber attacks can constitute an increasing threat for datareliant organizations such as NATO.

Beyond cyber defense, the Alliance started to work on the broader issue of Emerging Disruptive Technologies (EDTs) only in 2019, by setting up an innovation board co-chaired by the Deputy Secretary General and the Supreme Allied Commander Transformation. Moreover, a dedicated unit was created in the Emerging Security Challenge Division. Two White Papers were produced, respectively on AI and on autonomous weapons, to provide inputs for Allies’ decisions in this regard. The current NATO approach is based on the motto “adopting and adapting”, entailing five complimentary goals: (1) better understand emerging disruptive technologies; (2) properly look at their implications for defense; (3) decide about their use; (4) mitigate their risks; and (5) exploit their advantages.

Noticeably, the traditional defense industrial ecosystem entails long planning, oligopolistic supply and monopsonic demand. Over time, it was characterized by substantial technology transfers from the military to the civilian domain (the so-called ‘spin offs’), including the very same embryonic Internet. In recent years, several new technologies with relevant implications for security and defense have been emerging from a different ecosystem, marked by bottom-up innovation, a rapid development-to-market cycle, and a technology transfer from the civilian to the military domain. As a result, with the relevant exception of certain space assets and hypersonic technologies, the civilian sector is increasingly developing into the innovation driver, and defense one has become quite dependent. Such a shift implies that priority setting for current and future technology development is not substantially driven by states anymore. In the US, the Pentagon’s Defense Advanced Research Projects Agency (DARPA) struggles to develop a dialogue with the private sector gravitating around the Silicon Valley to embrace certain research lines. The NATO Industry Partnership on the cyber domain serves as platform for Alliance’s officials and industrial representatives to exchange notes, yet major ICT players do not seem very interested in having such a structured dialogue. Moreover, investments in these technologies require venture capitals and the acceptance of the risks to fail – something which usually states, and particularly Ministries of Defense, cannot afford. The US, the UK, France, Germany, the Netherlands and other Allies made certain steps to adapt their defense innovation models in these domains, but this is only the beginning of a long transformation process.

As a matter of fact, adapting to emerging and disruptive technologies is harder for some Allies than others. The related risk is moving towards a multi-layer Alliance, with some member states holding new technologies, and others not having such advantage. Ideally, the solution would be to collectively adopt certain new technologies, but this represents a challenge for the NATO Defence Planning Process, military procurement, common funding, etc. A technology group of experts has been appointed to reflect upon issues including but not limited to these, and the Secretary General will probably present a report to the next summit of Heads of state and governments.

#### NATO is uniquely vulnerable to hybrid threats---training builds cooperation and understanding to effectively counter impacts on decision-making

Hanna Smith 21, Director of Research and Analysis at the Centre of Excellence for Countering Hybrid Threats and visiting professor for the academic year 2020–2021 at the College of Europe, Bruges. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

Putting together the five characteristics of hybrid threats (use of multiple synchronized tools, ability to create ambiguity and to hide true intentions, deliberate threshold manipulation, exploitation of the seams of democratic societies, and use of decoys); the SEES model (situational awareness, explaining, estimating, and strategic notice); and the new challenges of today’s information environment (speed, volume, AI, and degrading expertise), they result in a mix that can influence decision-making algorithms and, in Omand’s words, “it is our own demons that are most likely to mislead us” (2020).

Since hybrid threats are designed to interrupt effectiveness of the SEES model at some point, by trying to create cognitive errors such as those arising from group thinking, 2 mirror imaging or applying unconscious confirmation bias, they can challenge organizations like the European Union (EU) and NATO even more than a state. The multilateral setting – with several, connected national interests – can be more vulnerable to hybrid threat activities. The things that can go wrong in the SEES model are especially vulnerable in a multilateral setting, unless there is a comprehensive approach, willingness to exchange information, joint understanding on resilience, and mechanisms to counter and respond in place.

The way Moscow and Beijing think about interference and influence is different from countries with a democratic system. For the EU and NATO, both Russia and China are difficult states to deal with. China is seen in the EU as a global partner, competitor and systemic rival. It has not been on NATO’s radar before the 2019 London Summit, but the Report “NATO 2030” delivered by the Group of Expert appointed by the Alliance’s Secretary General states that “NATO must devote much more time, political resources and action to the security challenges posed by China” (2020: 12). Russia has been viewed by the West as a systemic rival for much longer, but it has also been considered part of the European cultural heritage in the EU. For NATO, Russia has been the greatest military power in the East, which has conflicts of interest with NATO. For the moment, open military conflict is not viewed as very likely neither for Moscow nor for Beijing, although it is not excluded. This leaves the door open to hybrid threats, a mechanism that has roots in authoritarian strategic culture but also has national specificities. The things that can go wrong in the SEES model are challenged by the new information environment being manipulated according to the tactics of hybrid threats. Even if the EU is not a military alliance, while NATO is, both organizations are challenged in similar ways by hybrid threats. Given several factors, including overlapping membership, it is clear that weakening one will also weaken the other. Therefore, in the landscape of hybrid threats, the EU and NATO are considered as a united target by hostile actors – and they can also best counter and respond to these threats if working together.

Against this backdrop, here follow some recommendations aimed to policy-makers and expert communities in both NATO and EU countries: • The importance of analysis is growing. Too much effort has been put into collecting data, and not enough into training analysts. Older analysts need to be trained about the new information environment and its functioning. In turn, the younger generation needs to be trained on history, context and connections. Central elements in training are understanding the psychology of the adversary, the assessments of motivations, and rationales.

The cultural context of information is lost in the volume of information. International cooperation, especially on the part of an alliance like NATO, needs to be lifted to a new level. This does not only concern joint situational awareness about hostile actors, but also involves understanding partners and their perspectives. Without that mutual understanding among allies and partners, divergences can become over politicized and decision-making paralyzed, which is what the actors behind hybrid threats want.

There is a need for more effective training in the use of open-source intelligence, focusing on the sources and tools for finding information, including the biases they may have. In addition, more knowledge is needed to be able to detect linkages between actions. Hybrid threat activities start in a settled way, often on a very legal basis, and the potential for such activities to turn into hostile acts needs to be recognized.

Military communities should reach out more often to non-military expert communities. To counter hybrid threats, a multidisciplinary approach needs to be taken, which really means combining different disciplinary fields and expertise coming from practitioners, academics and the private sector.

Sharing the vocabulary is important when building situational awareness. Civil-military cooperation is needed here. The civilian side uses different words than the military and sometimes, even if the understanding of a concept would be shared, actors do not understand due to the use of different terms, and discussions can turn into an unnecessary battle of words.

#### Hybrid threats fueled by AI undermine decision-making and risk escalatory responses---effective NATO response is key

Sonia Lucarelli et al 21. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

Hybrid Threats to Allies’ Decision-Making. Hybrid threats is a broad category encompassing a variety of actors, actions and targets. As for actors, due to their actual capabilities, intentions and recent track records, China and Russia can be identified as the most gathering threats.

Concerning actions, information is key under several respects. It refers to Big Data and AI taken together, as the latter entails the use of algorithms to learn from the former with a view to exploit the target’s vulnerabilities. Digital connections are the underlying infrastructure used to perpetrate hybrid threats in the information domain. Western societies rely on virtual world platforms that can be targeted by potential attackers. Since global networks defy borders and limit state jurisdiction, they are harder to defend and allow potential attackers to act below the threshold of detection and attribution. Hybrid threats also benefit from the unprecedent speed and scope of information. This is not new in principle, but it has reached game-changing levels. On the one hand, managing this massive flow of information is just prohibitive for NATO and its member states; on the other hand, high speed of circulation translates into increased operational tempo.

Hybrid threats may take aim at a variety of targets, yet particularly concerning are offensive actions that might lead to societal polarization, elite disagreement and biased perceptions of foreign actors. These actions have the potential to affect decision-making at different levels, even undermining democratic states’ institutions. Accordingly, these hybrid threats could undermine decision-making process of Allies – and by reflex, NATO’s too. Decision makers face in particular three main set of problems when crafting a response to hybrid threats.

1) How to respond in non-escalatory ways? Since hybrid attacks exploit the grey zone to create ambiguity, including by manipulating the threshold of detection and granting plausible deniability, decision makers are faced with the risk of overreaction.

2) How to respond in democratic ways? Potential attackers may severely impair the decision-making process of democratic systems, putting under stress, for example, the constraint to abide by domestic and international law.

3) How to get public support? Since hybrid threats are usually covered or difficult to attribute, policy makers also have to persuade the public opinion of the very same existence of the threat.

#### Maintaining the lead in military AI strategy is key to preserving the balance of power, preventing runaway great power competition, and deterring Russian and Chinese attacks that escalate to nuclear Armageddon---creates space for political bargaining and diplomatic negotiations

Matthew Kroenig and Bharath Gopalaswamy 18, Matthew Kroenig is Associate Professor of Government and Foreign Service at Georgetown University and Deputy Director for Strategy in the Scowcroft Center for Strategy and Security at the Atlantic Council. Bharath Gopalaswamy is the director of the South Asia Center at the Atlantic Council. He holds a PhD in mechanical engineering with a specialization in numerical acoustics from Trinity College, Dublin. “Will disruptive technology cause nuclear war?” November 12. <https://thebulletin.org/2018/11/will-disruptive-technology-cause-nuclear-war> //pipk

Recently, analysts have argued that emerging technologies with military applications may undermine nuclear stability (see here, here, and here), but the logic of these arguments is debatable and overlooks a more straightforward reason why new technology might cause nuclear conflict: by upending the existing balance of power among nuclear-armed states. This latter concern is more probable and dangerous and demands an immediate policy response.

For more than 70 years, the world has avoided major power conflict, and many attribute this era of peace to nuclear weapons. In situations of mutually assured destruction (MAD), neither side has an incentive to start a conflict because doing so will only result in its own annihilation. The key to this model of deterrence is the maintenance of secure second-strike capabilities—the ability to absorb an enemy nuclear attack and respond with a devastating counterattack.

Recently analysts have begun to worry, however, that new strategic military technologies may make it possible for a state to conduct a successful first strike on an enemy. For example, Chinese colleagues have complained to me in Track II dialogues that the United States may decide to launch a sophisticated cyberattack against Chinese nuclear command and control, essentially turning off China’s nuclear forces. Then, Washington will follow up with a massive strike with conventional cruise and hypersonic missiles to destroy China’s nuclear weapons. Finally, if any Chinese forces happen to survive, the United States can simply mop up China’s ragged retaliatory strike with advanced missile defenses. China will be disarmed and US nuclear weapons will still be sitting on the shelf, untouched.

If the United States, or any other state acquires such a first-strike capability, then the logic of MAD would be undermined. Washington may be tempted to launch a nuclear first strike. Or China may choose instead to use its nuclear weapons early in a conflict before they can be wiped out—the so-called “use ‘em or lose ‘em” problem.

According to this logic, therefore, the appropriate policy response would be to ban outright or control any new weapon systems that might threaten second-strike capabilities.

This way of thinking about new technology and stability, however, is open to question. Would any US president truly decide to launch a massive, bolt-out-of-the-blue nuclear attack because he or she thought s/he could get away with it? And why does it make sense for the country in the inferior position, in this case China, to intentionally start a nuclear war that it will almost certainly lose? More important, this conceptualization of how new technology affects stability is too narrow, focused exclusively on how new military technologies might be used against nuclear forces directly.

Rather, we should think more broadly about how new technology might affect global politics, and, for this, it is helpful to turn to scholarly international relations theory. The dominant theory of the causes of war in the academy is the “bargaining model of war.” This theory identifies rapid shifts in the balance of power as a primary cause of conflict.

International politics often presents states with conflicts that they can settle through peaceful bargaining, but when bargaining breaks down, war results. Shifts in the balance of power are problematic because they undermine effective bargaining. After all, why agree to a deal today if your bargaining position will be stronger tomorrow? And, a clear understanding of the military balance of power can contribute to peace. (Why start a war you are likely to lose?) But shifts in the balance of power muddy understandings of which states have the advantage.

You may see where this is going. New technologies threaten to create potentially destabilizing shifts in the balance of power.

For decades, stability in Europe and Asia has been supported by US military power. In recent years, however, the balance of power in Asia has begun to shift, as China has increased its military capabilities. Already, Beijing has become more assertive in the region, claiming contested territory in the South China Sea. And the results of Russia’s military modernization have been on full display in its ongoing intervention in Ukraine.

Moreover, China may have the lead over the United States in emerging technologies that could be decisive for the future of military acquisitions and warfare, including 3D printing, hypersonic missiles, quantum computing, 5G wireless connectivity, and artificial intelligence (AI). And Russian President Vladimir Putin is building new unmanned vehicles while ominously declaring, “Whoever leads in AI will rule the world.”

If China or Russia are able to incorporate new technologies into their militaries before the United States, then this could lead to the kind of rapid shift in the balance of power that often causes war.

If Beijing believes emerging technologies provide it with a newfound, local military advantage over the United States, for example, it may be more willing than previously to initiate conflict over Taiwan. And if Putin thinks new tech has strengthened his hand, he may be more tempted to launch a Ukraine-style invasion of a NATO member.

Either scenario could bring these nuclear powers into direct conflict with the United States, and once nuclear armed states are at war, there is an inherent risk of nuclear conflict through limited nuclear war strategies, nuclear brinkmanship, or simple accident or inadvertent escalation.

This framing of the problem leads to a different set of policy implications. The concern is not simply technologies that threaten to undermine nuclear second-strike capabilities directly, but, rather, any technologies that can result in a meaningful shift in the broader balance of power. And the solution is not to preserve second-strike capabilities, but to preserve prevailing power balances more broadly.

When it comes to new technology, this means that the United States should seek to maintain an innovation edge. Washington should also work with other states, including its nuclear-armed rivals, to develop a new set of arms control and nonproliferation agreements and export controls to deny these newer and potentially destabilizing technologies to potentially hostile states.

These are no easy tasks, but the consequences of Washington losing the race for technological superiority to its autocratic challengers just might mean nuclear Armageddon.

#### Unrestrained great power competition causes extinction---China and Russia aren’t revisionist but the misperception of their own strength fueled by technological advances undermines climate negotiations and risks crises escalating to nuclear conflict---competition is inevitable but mitigating the risks of conflict through effective management and credible deterrence solves

Robert S. Litwak 21, Senior Vice President and Director of International Security Studies, Wilson Center. Dr. Litwak is also a consultant to the Los Alamos National Laboratory. He served on the National Security Council staff as director for nonproliferation in the first Clinton administration. He was an adjunct professor in the Security Studies Program at Georgetown University’s School of Foreign Service and has held visiting fellowships at Harvard University’s Center for International Affairs, the International Institute for Strategic Studies, the Russian Academy of Sciences, and Oxford University. "Geostrategic Competition and Climate Change: Avoiding the Unmanageable" September 15. <https://www.wilsoncenter.org/article/geostrategic-competition-and-climate-change-avoiding-unmanageable> //pipk

Humanity faces two catastrophic, indeed existential, threats—climate change and nuclear war. These risks play out before us as if on split screen. On one side are the here-and-now impacts of climate change: wildfires from Siberia to California to southern Europe, scorching “heat domes” over the Pacific Northwest, and “once in a thousand years” flooding in China. On the other, heightened geostrategic competition carrying the greatest risk of war between nuclear powers since the depths of the Cold War: in the month of April 2021 alone, a Russian troop surge on the Ukraine border triggered an “imminent crisis” alert in NATO while Chinese naval vessels and bombers conducted a largescale war-game encircling Taiwan. Though ostensibly discrete, the events playing out on the split screen are linked. This new nexus between geostrategic competition and climate change must be understood and integrated in policy if the twin threats are to be averted.

In his landmark book, Hot, Flat, and Crowded, New York Times columnist Thomas L. Friedman stated that the central challenge of climate change to humanity is now “to manage what is already unavoidable and avoid what will truly be unmanageable.” To that compelling formulation can be added a corollary reflecting the new nexus: avoiding unconstrained geostrategic competition is a prerequisite for managing the climate threat.

The window for humanity to avoid unmanageable climate change is narrowing. The United Nations’ Intergovernmental Panel on Climate Change (IPCC) reports that global temperatures will inexorably rise 1.5 degrees Celsius above pre-industrial levels by mid-century because of the projected level of atmospheric carbon. The IPCC starkly warns that the dire consequences arising from a temperature increase beyond that point can only be averted through prompt concerted global action to bend the curve and sharply reduce atmospheric carbon. UN Secretary-General António Guterres called the report a “code red for humanity.” China, the United States, and Russia are, respectively, the first, second, and fourth largest carbon emitters.

Yet at the precise historical juncture when unprecedented global cooperation is necessary to forestall catastrophe, the world is on the brink of unconstrained geostrategic competition. Indeed, U.S. relations with Russia and China are the worst they have been since the end of the Cold War, with a recent Department of Defense policy document warning of an “increased potential for regional conflicts involving nuclear-armed adversaries … and the potential for adversarial nuclear escalation in crisis or conflict."

One could logically argue against a linkage—that if the great powers have a mutual interest in averting a climate catastrophe then cooperation in that area could be compartmentalized from geostrategic tensions. But the onset of unconstrained geostrategic competition negates the possibility of compartmentalization. Contrasting positions on the nexus—the linkage between geopolitical competition and climate change—were evident in an exchange between Chinese Foreign Minister, Wang Yi and former Secretary of State John Kerry, now the Biden administration’s Special Presidential Envoy for Climate during his visit to China in August 2021. Wang warned that cooperation on climate change “cannot possibly be divorced” from other geopolitical tensions, while Kerry countered that climate change is neither “a geostrategic weapon” nor “ideological”….but “a global, not bilateral, challenge.”

These contending perspectives divide along political theorist Arnold Wolfers’s classic dichotomy between “possession goals” and “milieu goals.” Possession goals relate to the preservation or enhancement of a state’s narrow national interest—for example, in relation to territory or trade relations. In contrast, milieu goals pursued by a state aim to shape and improve the international political environment beyond parochial national interest—which in this context relate to the fostering of favorable conditions for concerted action on climate change.

Applying this framework, the Chinese Foreign Minister’s comment suggests that climate change is viewed within the context of furthering conventional Chinese possession goals—that cooperation on climate change can be leveraged to gain advantage on another issue (such as Taiwan). Kerry’s rejection frames climate change as a milieu goal whose existential stakes transcend any one state’s national interests. Through Kerry, the Biden administration has signaled its aspiration to eschew efforts by other states to relegate climate change to just another issue in transactional diplomacy.

Yet on a macro level—elevating climate change to a milieu goal—the linkage between geostrategic competition and climate change is unavoidable. Even if unconstrained geostrategic competition does not lead to conflict that might itself trigger catastrophic global destruction, virulent relations between the United States and its great-power adversaries create a political environment in which close cooperation on climate change becomes difficult, if not impossible. For that reason the avoidance of unconstrained geostrategic competition is a prerequisite for addressing climate change. To be sure, avoidance does not mean the elimination of geostrategic competition, but rather, bounding it to mitigate the risks of conflict through effective management.

Avoiding Unconstrained Competition

New risk factors have brought the great powers to the verge of unconstrained geostrategic competition. An understanding of those risks provides insight into how they can be mitigated and thereby managed.

A New Calculus of Risk

Contemporary geopolitics is driven not by Cold War ideology, but by nationalism and expansive assertions of state sovereignty. Nuclear powers are engaged in strategic competition with the United States over the territorial status quo in areas of vital interest—for China, Taiwan and the South China Sea; for Russia, Ukraine and the periphery of the former Soviet Union. This contrasts with the Cold War era in which the superpowers engaged in competition in the regions of what was then called the Third World, which were clearly of peripheral interest. This geostrategic competition runs the risk of war through inadvertent escalation driven by miscalculation and misperception.

The territorial dimension, which could be the occasion for great-power conflict, is compounded by key developments affecting the nuclear deterrent relationship between the United States and its great-power adversaries. All the nuclear-weapon states have embarked on ambitious force modernization programs, and they are developing capabilities, such as low-yield nuclear weapons, which critics warn make them more usable in a crisis. The Trump administration’s Nuclear Posture Review claimed that the Russians had adopted an “escalate to deescalate posture” involving the first use of tactical nuclear weapons. Moreover, military escalation has traditionally been conceived as progressing from conventional to nuclear forces. With the advent of new technologies, however, escalation during a crisis would most likely occur in a non-traditional domain—cyber or space. Conflict escalation could plausibly take the form of a cyberattack to interfere with an adversary’s communications with its nuclear systems or an attack on reconnaissance satellites to blind an adversary. These developments could have the destabilizing consequence of creating an incentive for one side or the other to take preemptive action during a crisis.

Managed Competition

The contemporary pursuit of strategic stability is conditioned by the recasting of the traditional tension between two Cold War dynamics. The first is the so-called “stability-instability paradox,” which captures the dynamic in which a nuclear stalemate between adversaries may embolden lower-level aggression on the regional level. The second is what Cold War strategist Albert Wohlstetter described as the “delicate balance of terror” which emphasized the maintenance of a stable and robust deterrence, thereby removing any incentive for one power or another to strike first in a crisis.

As during the Cold War, this tension can be managed, but it cannot be resolved. Key elements—some aspirational, others operational, many surrounded by uncertainty—will affect the prospects for successful management:

Resolve/Manage regional flashpoints—The best way to avoid conflict among nuclear-weapon states is to redouble diplomatic efforts to address the territorial disputes that could precipitate it. To be sure, if these territorial issues were easy to resolve, they would have been. In some instances, domestic politics in one or both parties may be an impediment to resolution; in others, the discrete territorial issue may be a proxy for a more deeply rooted source of enmity or grievance. If resolution is not possible, conflict management may be. For example, the Code for Unplanned Encounters at Sea (CUES), to which both China and the United States are signatories, may be a mechanism for managing maritime tensions between their navies.

Maintain the residual arms control architecture—The new START treaty has been extended until 2026 and provides certainty and time for Russia and the United States to agree on a successor arrangement and outstanding issues (such as non-strategic nuclear weapons and engaging or taking Chinese capabilities into account).

Do not blur conventional and nuclear operations to prevent inadvertent escalation—Placing conventional warheads on ballistic missiles, such as that envisioned through the “Conventional Prompt Global Strike,” has utility (the ability to reach any target on the globe in under one hour), but runs the risk that Russia may perceive (and respond to) the launch of a ballistic missile that it associates with U.S. nuclear capabilities as the initiation of such an attack. Another potential driver of inadvertent escalation, with implications for both Russia and China, is the targeting of an adversary’s conventional capabilities that are co-located with its nuclear capabilities.

Mitigate risks through strategic dialogue—In the absence of an arms control architecture, each nuclear power in the multipolar system will have strategic autonomy to structure its offensive and defensive systems. All of the nuclear-weapon states have long been uncomfortably ambivalent with vulnerability captured in the acronym MAD—mutual assured destruction. But since the Cuban missile crisis, assured retaliation—eliminating incentives for a surprise first strike—has been the sine qua non of strategic stability. The risk now is that an unconstrained arms race (unregulated numbers of offensive and defensive systems, in tandem with new weapons technologies and cross-domain threats to space and cyber assets) could revive those incentives and undermine the deterrent relationships. In the past, arms control negotiations provided a forum for strategic discourse. “On a bilateral or a multilateral basis,” scholars Christopher Chyba and Robert Legvold argue, “the United States, Russia, and China should pursue discussions intended to improve understanding of one another’s strategic concerns and views on which actions by an adversary would be especially concerning or dangerous.” The focus should be on negotiated restraints (e.g., a ban on the deployment of anti-satellite weapons) to enhance stability and reduce incentives for one side or the other to act preemptively during a crisis.

Managing the Geopolitics of Climate Change

When George Kennan, the diplomatic architect of U.S. containment policy, declared the end of the Cold War, he explained that the Soviet Union under Mikhail Gorbachev had evolved from a revolutionary state into an orthodox great power—the country “should now be regarded essentially as another great power, like other great powers.” Kennan was essentially arguing that Russia’s post-Soviet foreign policy, stripped of ideology, was a renationalized version of traditional Russian foreign policy with strategic priorities starting with the “near abroad” of the former Soviet republics abutting the West.

A “risen” China presents an analogous case of an orthodox great power making assertive claims of territorial sovereignty on its periphery. This new superpower is deeply integrated into the global economy and presents a variegated challenge in a way that Russia, a one-dimensional superpower, does not. War between the United States and China is not inevitable, but the world’s two dominant powers could mismanage their way into it.

That Russia and China are orthodox great powers, not revolutionary states seeking the overturn of the international order, creates political space for the United States to initiate strategic dialogues with them separately or together to lower tensions and reduce the risks of conflict—thereby fostering a favorable international milieu to address the exigencies of climate change.

### Advantage Two---Cooperation

#### The aff spills over to broader international democratic cooperation on AI

Ulrike Esther Franke 21, senior policy fellow at the European Council on Foreign Relations (ECFR). She leads ECFR’s Technology and European Power initiative. Her areas of focus include German and European security and defence, the future of warfare, and the impact of new technologies such as drones and artificial intelligence on geopolitics and warfare. PhD in International Relations from the University of Oxford. Franke is a policy affiliate at the Governance of AI project at Oxford University’s Future of Humanity Institute. "Artificial divide: How Europe and America could clash over AI" – ECFR/367 2. January. <https://ecfr.eu/wp-content/uploads/Artificial-divide-How-Europe-and-America-could-clash-over-AI.pdf> //pipk

A glance at the history of artificial intelligence (AI) shows that the field periodically goes through phases of development racing ahead and slowing down – often dubbed “AI springs” and “AI winters”. The world is currently several years into an AI spring, dominated by important advances in machinelearning technologies. In Europe, policymakers’ efforts to grapple with the rapid pace of technological development have gone through several phases over the last five to ten years. The first phase was marked by uncertainty among policymakers over what to make of the rapid and seemingly groundbreaking developments in AI. This phase lasted until around 2018 – though, in some European states, and on some issues, uncertainty remains. The second phase consisted of efforts to frame and AI challenges politically, and to address them, on a domestic level: between 2018 and 2020, no fewer than 21 EU member states published national AI strategies designed to delineate their views and aims, and, in some cases, to outline investment plans.

The next phase could be a period of international, and specifically transatlantic, cooperation on AI. After several years of European states working at full capacity to understand how to support domestic AI research, including by assembling expert teams to deliberate new laws and regulations, there is growing interest among policymakers and experts in looking beyond Europe. On the EU level, AI policy and governance have already received significant attention, with the European Commission playing an important role in incentivising member states to develop AI strategies, such as by starting to tackle issues around how to make sure AI is “ethical” and “trustworthy”. But recent months have seen a rise in the number of calls for international cooperation on AI driven by liberal democracies across the world. Western countries and their allies have set up new forums for cooperation on how to take AI forward, and are activating existing forums. More such organisations and platforms for cooperation are planned.

Calls for cooperation between the United States and Europe have become particularly regular and resonant: following last year’s US presidential election, it was reported that the European Commission planned to propose a “Transatlantic Trade and Technology Council”, which would set joint standards on new technologies. And, in September 2020, the US set up a group of like-minded countries “to provide values-based global leadership in defense for policies and approaches in adopting AI”, which included seven European states, in addition to countries such as Australia, Canada, and South Korea. In June 2020, the Global Partnership on Artificial Intelligence was founded to consider the responsible development of AI; it counts among its members the US, four European states, and the European Union.

This paper examines the reasons European states may want to work with the US on AI, and why the US may want to reach out to Europe on the issue. It also identifies the points of disagreement that may stop the allies from fully fleshing out transatlantic AI cooperation. The paper shows that, while both sides are interested in working together, their rationales for doing so differ. Furthermore, economic and political factors may stand in the way of cooperation, even though such cooperation could have a positive impact on the way AI develops. The paper also argues that transatlantic cooperation in the area of military AI could be a good first step – here, Europe and the US should build on existing collaboration within NATO. The paper concludes with a brief discussion of the different forums that have been created or proposed for transatlantic and broader Western cooperation on AI.

#### International cooperation key to prevent authoritarian AI from crushing democracy worldwide

Andrew Imbrie et al 20, Andrew Imbrie Ryan Fedasiuk Catherine Aiken Tarun Chhabra Husanjot Chahal. Center for Security and Emerging Technology (CSET) at Georgetown’s Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. February. "Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI" //pipk

How can the United States collaborate with allies and partners to shape the trajectory of artificial intelligence in ways that will promote liberal democratic values and protect against efforts to wield AI for authoritarian ends?

This question is both important and urgent. It is important because America’s broad network of alliances and security partnerships is a singular asset in defending liberal values. It is urgent because China, Russia, and other authoritarian powers seek to achieve strategic advantage through AI and the export of censorship and surveillance technologies to countries across the globe.1 By one estimate, more than 100 countries purchase surveillance and censorship gear from China and Russia, receive training on these technologies, or simply imitate methods of surveillance and censorship that are designed to control public opinion and stifle dissent.2

As the digital and physical environments become intertwined, authoritarian practices in one domain will increasingly encroach upon the other. At stake are the core values of liberty, equality, and justice that underpin free and open societies. All democratic nations must work together to uphold basic principles, set international rules of the road, and articulate a positive vision for the future in the age of AI.

Within the United States, and certainly within allied countries, debate persists over the threat of digital authoritarianism and how to counter it. While U.S. allies will likely vary in their strategic orientations toward China and Russia, there is a growing consensus on the need to showcase a democratic way of AI. These debates will take shape in a world of globalized markets for AI talent and integrated supply chains. In this context, the right U.S. approach would leverage its network of allies and partners to safeguard democracy and liberal values. An alliance-centric strategy provides a competitive advantage over any single country that attempts to develop a robust AI ecosystem on its own.

The United States and its allies should play to their strengths. This positive agenda begins with shaping the ecosystems for the development and deployment of safe and reliable AI. The most effective approach would capitalize on advances in AI and machine learning to foster sustainable and inclusive economic growth, improve service delivery, and promote transparent and accountable governance. The United States and its allies should pursue a vision of the future in which AI enables strengthened data privacy standards and respect for civil liberties; economic empowerment of citizens within rules-based market economies; cleaner, safer, and more efficient transportation; precision medical diagnosis; greater access to education; and more effective disaster response.

#### Democracy solves extinction

Carla Zoe Cremer & Luke Kemp 21, The Future of Humanity Institute, Oxford. Centre for the Study of Existential Risk, Cambridge. "Democratising Risk: In Search of a Methodology to Study Existential Risk" <https://arxiv.org/ftp/arxiv/papers/2201/2201.11214.pdf> //pipk

There is an intimate and neglected relationship between existential risk and democracy. Democracy must be central to efforts to prevent and mitigate catastrophic risks. It is also an antidote to many of the problems manifest in the TUA. Do those who study the future of humanity have good grounds to ignore the visions, desires, and values of the very people whose future they are trying to protect? Choosing which risks to take must be a democratic endeavour.

We understand democracy here in accordance with Landemore as the rule of the cognitively diverse many who are entitled to equal decision-making power and partake in a democratic procedure that includes both a deliberative element and one of preference aggregation (such as majority voting)45,115. Decision-making procedures are not either democratic or non- democratic, but instead lie on a spectrum. They can be more or less democratic, inclusive, and diverse.

We posit three reasons for why we should democratise research and decision-making in existential risk: the nature of collective decision-making about human futures, the superiority of democratic reason, and democratic fail-safe mechanisms.

Avoiding human extinction, or crafting a desirable long-term future, is a communal project. Scholars of existential risk who take an interest in the future of Homo sapiens are choosing to consider the species in its entirety. If certain views are excluded, the arguments for doing so must be compelling.

Democracy will improve our judgments in both the governance and the study of existential risks. Asking how our actions today influence the long-term future is one of the most difficult intellectual tasks to unravel, and if there is a right path, democratic procedures will have the best shot at finding it. Hong and Page116,117 demonstrate both theoretically and computationally that a diverse group of problem-solving agents will show greater accuracy than a less diverse group, even if the individual members of the diverse group were each less accurate. Accuracy gains from diversity trump gains from improving individual accuracy. Landemore115, builds on this work to advance a probabilistic argument that inclusive democracies will, in expectation, make epistemically superior choices to oligarchies or even the wise few. This is supported by promising results in inclusive, deliberative democratic experiments from around the world 118. In the long run, democracies should commit fewer mistakes than alternative decision-making procedures. If this is true, it should improve the accuracy of research efforts and decision-making. We are more likely to make accurate predictions about the mechanisms of extinction, probable futures, and risk prevention if the field invites cognitive diversity, builds flat institutional structures, and avoids conflicts of interest.

Thereare many ways to consider the interests of the many. Democratic assemblies could allow global citizens to deliberate about the futures they prefer, citizens could be surveyed, and the field of ERS itself could be diversified. At the moment, the field is, as many academic disciplines are, unrepresentative of humanity at large and variably homogenous in respect to income, class, ideology, age, ethnicity, gender, nationality, religion, and professional background. The latter issue is particularly true of existential risk, which, despite being an inherently interdisciplinary endeavour, is at the highest levels dominated by analytic moral philosophers. We need to be vigilant to what perspectives are not represented in the study of existential risk. An awareness of bias will go some way towards mitigating its negative effects. To get close to replicating the cognitive diversity found among humans, we must begin by inviting different thinkers with different values and beliefs into the field.

Democracies can limit harms. Any approach to mitigating existential threats could create response risks, and the TUA seems particularly vulnerable to this. Despite good intentions and curiosity-driven research, it could justify violence, dangerous technological developments, or drastically constrain freedom in favour of (perceived) security. If we hope to explore ideas but minimise harms, democracies can be used to moderate the measures taken in response to harmful ideas. It seems, for example, vanishingly unlikely that a diverse group of thinkers or even ordinary citizens would entertain the idea of sacrificing 1 billion living, breathing beings for an infinitesimal improvement in reaching an intergalactic techno-utopia. In contrast, the TUA could recommend this trade-off.

The democratic constraint of extreme measures may simply be a form of collective selfinterest. Voters are unlikely to tolerate global catastrophic risks (GCRs), which incur the death of a sizeable portion of the electorate, if they know they themselves could be affected. We expect that scholars who do not support sacrificing current lives in the name of abstract calculations, but would still like to explore the use of expected value theory in existential risk, will be in support of democratic fail-safe mechanisms.

Empirically, this fail-safe mechanism seems to work. Even deeply imperfect democracies, like the ones we inhabit now, often avert detrimental outcomes. Democracies prevent famines 119 (although not malnutrition)120. They make war — a significant driver of GCRs — less likely 121. The inclusion of diverse preferences in democracies, such as those achieved through women’s suffrage, further decreases the likelihood of violent conflict 122. Citizens often show a significant risk aversion in comparison to their government. While surveys are notoriously difficult to collect and interpret, existing data suggest that the public has little support for nuclear weapons use 123–125, but strong support for action against climate catastrophe 126–128. We can further show that when citizens deliberately engage with the subject at hand, their concern and readiness for action often increases 118. For example, citizen assemblies on climate change have recommended widespread policy-changes across sectors, amendments to incentive structures and laws against ecocide to reach emissions targets 129. Indeed, many lament that when it comes to genetically modified organisms and nuclear power, citizens are far too riskaverse130 . The problem is not that the public is riddled with cognitive biases that make them unconcerned about global catastrophes.

Democratic debate cannot be an afterthought. Navigating humanity through crises will involve many value-laden decisions under deep uncertainty. Democratic procedures can deal with such hard choices. Greater cognitive diversity should be represented amongst scholars of ERS. Recommendations on policies that would reduce risk should be passed through deliberative assemblies and await the approval of a wider pool of ordinary citizens, as they will be the ones who will bear this risk. A homogenous group of experts attempting to directly influence powerful decision-makers is not a fair or safe way of traversing the precipice.

#### Global cooperation on AI generates governance capacity necessary to prevent worst-case scenarios

Yves Tiberghien et al 22, professor of political science and director emeritus of the Institute of Asian Research, University of British Columbia. Danielle Luo, senior analyst, international public affairs at CPP Investments. Panthea Pourmalek is a master of public policy and global affairs student at the University of British Columbia. "Existential Gap: Digital/AI Acceleration and the Missing Global Governance Capacity" February 14. <https://www.cigionline.org/articles/existential-gap-digitalai-acceleration-and-the-missing-global-governance-capacity/> //pipk

We are facing an ever-growing gap between the phenomenal acceleration of technology and of connectivity, and the human capacity to manage these trends. The gap is well-documented in the fields of finance, climate change, pandemics and nuclear risks. But the contrast between the exponential growth of disruptive technology and the lacklustre supply of governance mechanisms is starkest in the fields of digital governance and artificial intelligence (AI).

That gap becomes existential when we consider the likely future development of artificial general intelligence (AGI) (Ord 2020) or superintelligence (Bostrom 2015) that can be misaligned with human values or even the goal of ensuring the continuity of human existence. This question of the governance of life with AI may be the most essential question of our time (Tegmark 2017), but you would not know it from the current output of global governance in this field. Summarizing the judgement of many scientists in the field, Toby Ord argues that unaligned AGI is actually the number-one global existential risk for humanity, with a 10 percent chance of human extinction within 100 years. The prophesized existential threats posed by extreme and accelerated technological advancement and expansion have never been as close to reality as they are now. As noted by Yuval Noah Harari and Daniel Kahneman (2021) in a recent conversation, the task of taming and governing the digital/AI revolution is daunting. Humanity may have no slack for a mistake this time around, given the existential consequences of such a mistake.

Today, we already benefit from tremendous digital or AI innovations in e-commerce, social media and communication, home management, work, health care, education, transportation, and entertainment (West and Allen 2020). We can foresee that AI-driven algorithms may soon be able to correct human judgement flaws (or noise) caused by fatigue, irregularity, emotions and other weaknesses, afflictions that can generate variation in decisions by up to 50 percent (Kahneman, Sibony and Sunstein 2021). Within two decades, we can envisage a world with generalized deep learning and virtual reality, computer vision, contactless love, fully autonomous vehicles in most advanced and emerging economies, autonomous weapons in militaries and a dream of plenitude (Lee and Chen 2021).

Yet, today, we witness tremendous havoc created by the explosion of social anger, exacerbated by sophisticated social media algorithms, deep polarization, the return of tribal politics, the loss of agreed truths and the spread of misinformation and dangerous conspiracies, the loss of privacy, the rise of massive and uber-powerful tech companies, and massive job displacement and inequality (Bartlett 2018). Influence operations by foreign states have also amplified such social anger and polarization in many democracies, adding a degree of external threat and urgency. We also live with a world of security-driven digital decoupling between the United States and China (Ma 2021). In other words, the digital revolution is moving faster than the human capacity to cope with it, embed it within a public good-oriented framework and steer its disruptive power toward a non-destructive direction.

The problem is visible at the national level but particularly salient at the global level. Digital/data governance is fragmenting among at least four poles: a US model with maximum innovation and limited regulation; an EU model with a strong regulatory balance; an India model with an emphasis on digital sovereignty and infant industry protection (applicable to other developing countries); and a Chinese model with both rapid innovation, strong state control and surveillance. Our global governance capacity is affected by multiple splits: a US-EU split over privacy, tax and anti-monopoly regulations; an India-West split over data ownership and first-mover advantage; and, worst of all, a potential digital cold war between the United States (and its allies) and China. In response to this dire need for governance, Rohinton P. Medhora and Taylor Owen (2020) have proposed a need for a new fundamental effort at coordinated governance — or a “digital Bretton Woods.” While fundamental international conditions and global distribution of power today differ drastically from the Bretton Woods era, a high-stake and fragmented digital world is in dire need of such renewed cooperative spirit.

Recognizing the gap in digital governance, we ask the following questions: What is the scale of the gap in governance relative to requirements needed to keep the digital economy afloat? And what could be a pathway forward in the context of the growing securitization and increasing divides?

It is urgent to raise a sense of awareness, mobilize all social and public actors around this urgent dilemma and catalyze a multi-level effort to address this conundrum. We argue that no global, regional or national institution alone will be able to deliver the right governance capacity. Instead, we recommend a highly reactive, innovative and competitive model of networked governance that operates at multiple levels with key nodes and catalysts.

Governance innovation must keep pace with technological innovation. Given how far the digital cold war has already proceeded and the currently low capacity to cooperate between the United States and China, part of the solution will need to involve clubs and alliances of countries and non-state actors. At the same time, some level of global coordination and basic rules for global co-existence are crucial for success in managing this existential threat. The Group of Twenty (G20) is one critical venue for such work, even though it has not delivered so far.

Key Indicators on the Exponential Rise of the Digital Economy

Over the last few years, and particularly during the COVID-19 pandemic period, the digital economy has experienced an exponential rise and begun to transform human interactions, production and trade (Suominen 2019). In Table 1, we offer a review of selected indicators on cross-border data flows and digitalization. It is clear that digital trade and cross-border data flows, along with other digital innovations, are rising faster than physical trade flows.

Table 1: Summary of Key Indicators on the Explosion of the Digital Economy

TLP\_Table1.png

Sources: Data on cross-border data flows retrieved from TeleGeography; Data on e-commerce as a % of global GDP derived from global e-commerce value and global GDP; global e-commerce value data retrieved from Insider Intelligence; global GDP data retrieved from World Bank; data on cross-border mobile payments retrieved from GSMA; data on AI economy size retrieved from Fortune Business Insights; data on self-driving cars growth trend retrieved from Facts and Factors Research; data on facial recognition growth trend retrieved from Emergen Research. Note: Numbers with an asterisk are projected data.

Table 1 shows that key components of the digital economy, including e-commerce, AI economy and cross-border mobile payments, have experienced steady growth since 2017, and are projected to continue growing. 2020 saw the sharpest growth in several components, likely due to mobility constraints and increased reliance on digital tools associated with the COVID-19 pandemic. While current data illustrates useful trends, it is important to note that the volume of digital trade — a key component of data on the digital economy — is very hard to measure.1 This is in part due to the lack of a shared definition of what constitutes digital trade, highlighting a need for technocratic standardization as a basis for high-level digital governance.

Why Addressing the Digital Governance Gap Matters

We offer here a typology of risks involved in the digital governance gap:

Under-institutionalized markets (North 1990; Williamson 1985): All markets require basic rules and governance to ensure trust, accountability and resilience, and to prevent abuse by potential oligopolistic players. Global markets require global institutions. Digital governance is a new domain, where innovators and disruptors have been able to run ahead of rule making. We are emerging from more than two decades of an under-institutionalized digital economy, in which many large imbalances and market deficiencies are appearing in every society around the world.

Unprecedented power of digital companies: The current moment may be the first time in human history that a private company such as Facebook (Meta) has the ability on its own to screen messages of leaders and politicians from every country in the world, except China, North Korea, Cuba, and maybe Iran. And this global function is only peripheral to Facebook’s core business, with just hundreds of assigned staff. In other words, Facebook, along with Twitter and a couple more giant for-profit digital companies, has acquired in less than 15 years the power to control information, emotions, narratives and political/social mobilization in the majority of countries of the world, including the United States. And they are generating disproportionate profits from this dominant position. All this is taking place in a near complete vacuum of digital governance. Most countries outside the United States and China have limited power to regulate and control these US-based and China-based global digital companies. The US government retains residual power to do so, but has been unable to act due to constitutional constraints and great polarization in Congress. China (behind its internet firewall) has already started wrestling with this power and cracking down on its own giants. India has started to pass restricting measures on the power and freedom of social media companies on its territory. The European Union is taking its own regulatory path through the General Data Protection Regulation (GDPR) and its successor currently under negotiations, as well as tough competition rules, within the constraints of its relative weak position in the space (no EU-based digital giants). But the governance gap remains enormous in the United States and many other countries, as well as at the global level.

Risk of explosive social disruptions and inequality: The scale of disruption induced by digital and AI innovation under current intellectual property protection and lack of redistribution accrues immense winner-take-all benefits to first movers. We are witnessing at the same time a historic concentration of capital and wealth and growing numbers of displaced or laid-off workers in declining industries. We can soon expect to have digital entrepreneurs with a net worth of US$1 trillion (from a quarter of a trillion so far with Elon Musk and Jeff Bezos), alongside massive job displacement. Such fast-paced social dislocation and inequality could prove politically explosive and very hard to manage (Lee 2018). No social system is ready — and the global governance is not ready either. The viability of modern states is also at stake, as their revenue base keeps eroding. In the late nineteenth century, when the oil and railroad revolutions generated a similar concentration of wealth, it took all the power and energy of a Teddy Roosevelt to tame these forces. We don’t have such capacity today.

Global systemic risks: The global digital economy is extraordinarily interconnected and fast-paced. It encompasses data flows, e-commerce, mobile payments, digital currency (with increasing future prevalence), AI algorithms, fully automated cars and weapons. Is the current system resilient against contagion effects or collapse? What is the safety net in case of a crisis?

Loss of privacy and potential loss of human freedom: The rise of the surveillance state is an extreme reality in China, including in repression operations. But it is also a reality all over the world. Companies such as Google and Facebook not only have more data about each individual than they can imagine, but also the capacity to couple this data with future AI algorithms for all kinds of usage. For the first time in human history, most humans have handed over fundamentally private information to either giant private actors, states or both. Even worse, regulatory breaches (cf. Cambridge Analytica) give political or criminal actors access to important and strategic data, with which they can manipulate human psychology.

Democratic existential crisis: The explosion and equalization of information, and the intensification of complexity, have eroded any sense of agreed truth and reality within most nations. Social media has unexpectedly accelerated polarization, amplified echo chambers and closed loops among like-minded individuals, greatly contributing to extreme polarization in many societies across the planet. Absurd conspiracies can spread virally and inspire violent actions by large spontaneous groups, as shown by the January 6 insurrection in the United States (with a large number of people mobilized by QAnon beliefs). At a deeper level, new understandings about the concept of extended mind in psychology show that humans are increasingly delegating part of their thinking processes to smart phones and their algorithm-driven suggestions devised to serve profit-seeking companies (cf. work by Peter Reiner).2 Human behaviour may be profoundly changing in ways never seen before, which our democratic institutions are not ready for. Facebook’s move to a metaverse world that can attract humans to spend time and to be transformed in a totally unregulated environment has the potential to further increase this risk.

External cyberthreats to democracy: The current digitalized world is also increasingly used as a tool to undermine democracy from the outside. Russia’s interference in the 2016 American presidential election through social media campaigns highlights the extent to which an unregulated digital sphere could undermine democratic institutions. China’s propaganda efforts on platforms such as Twitter and YouTube during the 2020 Taiwanese presidential election are yet another example that an unregulated cyberspace could warrant injudicious digital campaigns. More recently, the sale of Israeli spyware Pegasus to various governments — who in turn used it for malicious efforts against other states, and individuals such as journalists, reporters and human rights activists.

Rise of cybercrimes, cyberpiracy and cyberattacks (Deibert 2013, 2020; Sanger 2018). The open structure of the internet has left great space for hackers and organized gangs. Worse, the existence of an illegal black market incentivizes smart young digital talents in many places around the world to look for zero-day loopholes in operating systems and sell those to the highest bidders, including the national security agencies of many countries (Perlroth 2020). This quickly escalates into a growing cyberspying competition and even cyberwar (Segal 2016).

Fragmentation of the internet and of the digital economy into rival spheres (splinternet), and weaponization of interdependence (Drezner, Farrell and Newman 2021; Farrell and Newman 2019; Ma 2021; Suominen 2019). The raising of stakes in the digital economy, the sudden acceleration of the digital transformation in China, the intensification of security competition and the high prevalence of dual-use technologies in the digital/AI space have led to an increasing potential for a digital cold war, as well as other fractures among various regional poles. As Winston Ma (2021, 42) writes: “all in all, U.S.-China tech decoupling is real and accelerating. Hence, the digital economy is in a vital conflict and crisis: the global tech world, together with at least part of the world economy, is now fractured into two-and potential more…spheres of influence, whereas tech entrepreneurs are driving the prospect of a technological singularity, hyper-connected society, and internet of everything.” This decoupling is extremely risky, because it is abrupt, driven by fears and not negotiated. It leads to highly explosive tit-for-tat measures that are hard to contain. This process massively interferes with the human effort to generate a global governance framework.

Measuring the Digital Global Governance Gap

In Table 2 (and, in greater detail, in Annex 1), we offer a summary of existing digital governance at the global, regional, club or national levels. Overall, we evaluate that the governance of basic internet functions remains surprisingly resilient (8/10), but other dimensions of digital and AI governance are extremely weak (2/10 in most cases).

One powerful indicator that highlights the gap between the risks outlined above and the current state of global governance is found in the recent G20 Rome Leaders’ Declaration. The focus remains on sharing the gains of digital innovation for the green economy, education and economic growth. However, the digital economy gets only brief mentions toward the latter part of the declaration with generic and toothless statements such as the following:

“In cooperation with social partners, we will adopt human-centered policy approaches to promote social dialogue and to ensure greater social justice; safe and healthy working conditions; and decent work for all, including within global supply chains. To reduce inequalities, eradicate poverty, support worker transitions and reintegration in labour markets and promote inclusive and sustainable growth, we will strengthen our social protection systems” (G20 Leaders 2021, para. 35).

“We recognize the role of technology and innovation as key enablers for the global recovery and sustainable development.…With this in mind, we will work to strengthen bilateral and multilateral cooperation to secure our ICT, address shared vulnerabilities and threats, and combat cybercrime” (ibid., para 46).

“Well aware of the benefits stemming from the responsible use and development of trustworthy human-centered Artificial Intelligence (AI), we will advance the implementation of the G20 AI Principles” (ibid., para 47).

“We will also continue to further common understanding and to work towards identifying commonalities, complementarities and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust, in order to foster future interoperability. Recognizing the responsibility of digital service providers, we will work in 2022 towards enhancing confidence in the digital environment by improving internet safety and countering online abuse, hate speech, online violence and terrorism while protecting human rights and fundamental freedoms” (ibid., para. 48).

This summary of current global digital governance reveals the extent of the gap with what is at stake!

Table 2: Evaluation of What We Have and of the Gap to a Functional Global System, under Conditions of Securitization and Great Power Rivalry

TLP\_Table2.png

Source: Authors. Notes: ASEAN = Association of Southeast Asian Nations; CARICOM = Caribbean Community; CPTPP = Comprehensive and Progressive Agreement for Trans-Pacific Partnership; DEPA = Digital Economy Partnership Agreement; ECOWAS = Economic Community of West African States; FAANG = Facebook, Amazon, Apple, Netflix and Alphabet (formerly Google); ICANN = Internet Corporation for Assigned Names and Numbers; NATO = North Atlantic Treaty Organization; OECD = Organisation for Economic Co-operation and Development; OIE = World Organisation for Animal Health; SADEA = Singapore-Australia Digital Economy Agreement.

From Table 2, we can draw several important lessons. First, the well-established nature of internet governance shows that governance in the digital domain is indeed possible. Internet governance was established several decades ago and is operated by largely independent and apolitical entities. However, times have changed. It is important to recognize the current geopolitical stakes and inherent international context that now constitutes multi-polarities of interest. Second, despite the absence of a centralized governance mechanism for digital trade, the language and framing of rules on digital trade as expressed in recent free-trade and digital partnership agreements are increasingly similar, and indicate some degree of convergence in the governance of digital trade. Finally, the domain that fairs most poorly in terms of governance is also the domain that is most politicized. The primary motivation behind limited alignment on accepted 5G or semiconductor providers is driven by the US geopolitical push against Chinese 5G giant Huawei and semiconductor giant SMIC, risking bifurcation in global standards and encouraging autarkic behaviours such as the EU idea of “chips self-sufficiency.”

As a reference, Table 3 offers a comparative summary of different approaches used by the United States, European Union, China and India. For a more detailed look at key legislation shaping digital governance in each jurisdiction, refer to Annex 2.

Table 3: Four Competing Approaches to Digital Governance

TLP\_Table3.png

Conclusion and Global Digital Governance Proposals

There is a huge disconnect between the speed of technological development, the scale of existential risks involved, and the acceleration of securitization on the one hand and the supply of national/global governance and increase in human capacity on the other hand.

Political leaders are not yet incentivized to deal with this existential set of issues. They are distracted by short-term political urgencies and the acceleration of tit-for-tat rivalry.

A digital Bretton Woods captures the spirit of global digital governance we should strive for. However, it is essential to recognize the radically different context of today compared to 1944. The lack of “global yearning for peace and stability” highlighted by Medhora and Owen (2020), is further aggravated by a new environment of multi-polarity and diffused interests. Thus, we may only be able to reach a thin global framework under current geopolitical conditions, and it can only be part of a larger multi-level and partly competitive effort to generate governance capacity.

The human solutions to the predicament cannot come from a single locus or look like responses to past governance issues. There will need to be multiple entry points with a networking and competitive dynamic among them — some from the G20, World Trade Organization (WTO), United Nations, some from club governance (Group of Seven [G7], Quad, China-based solutions, along with bilateral forums such as the US-EU dialogue), and some from private actors, civil society networks, think tanks and academic actors.

For any critical mass process of capacity development to occur in such a way, both catalyzing focal points and elements of coordination will be required. The global level may yet play a key signalling role or allow minimum convergence on dimensions of common interest. The G20 urgently needs an upgraded high-level working group on all digital governance questions.

### Plan

#### The United States federal government should substantially increase its artificial intelligence military logistics pilot projects with the North Atlantic Treaty Organization

### Solvency

#### Starting with an AI logistics pilot through NATO is key---it’s key to military effectiveness, is technologically and politically feasible, and establishes benchmarks necessary for effective AI testing and standards necessary for innovation and interoperability---allies only say yes to the plan

Margarita Konaev & Husanjot Chahal 21, Research Fellow & Research Analyst, Center for Security and Emerging Technology, Georgetown University. "The Path of Least Resistance Multinational Collaboration on AI for Military Logistics and Sustainment" April. <https://cset.georgetown.edu/wp-content/uploads/CSET-Path-of-Least-Resistance.pdf> //pipk

Focusing on AI-enabled Military Logistics and Sustainment In military affairs, logistics is tasked with managing the global supply chain for the armed services, including “the transfer of personnel and materiel from one location to another, as well as the maintenance of that materiel.”27 Sustainment is a broader term, encompassing logistics as well as financial management, personnel services, and health services which together provide the support necessary to maintain operations until the mission is accomplished.28 The two functions are closely intertwined. NATO’s Allied Joint Doctrine for Logistics, for instance, offers a comprehensive definition of logistics that also entails elements of sustainment, encompassing the aspects of military operations that deal with “design and development, acquisition, storage, movement, distribution, maintenance, evacuation and disposition of materiel; transport of personnel; acquisition, construction, maintenance, operation and disposition of facilities; acquisition or furnishing of services; and medical and health service support.”29

Logistics and sustainment are essential to military effectiveness, readiness, survivability, and endurance, and in many ways, constitute the lifeblood of military power.30 The Department of Defense, in turn, sees great promise in leveraging AI/machine learning (ML) technologies for military logistics and sustainment to better maintain equipment, reduce operational costs, and improve readiness. The Department of Defense’s AI strategy, for example, includes efforts related to AI-enabled logistics and sustainment, such as “implementing predictive maintenance and supply, and streamlining business processes,” as part of its strategic approach to “delivering AI-enabled capabilities that address key missions.”31 Joint Logistics, in turn, is one of the JAIC’s key mission initiatives, dedicated to “improving fleet readiness through AI-driven diagnostics, training, process improvements, demand forecasting, and supply chain optimization.”32

The discussion below outlines the technological, political, and strategic imperatives and opportunities for multinational collaboration on AI-enabled military logistics and sustainment. Naturally, the principal mission of militaries is national defense and the force (including logistics and sustainment functions) must be prepared for combat at any time. Modern militaries, however, are massive organizations that employ hundreds of thousands of people, if not more. The Department of Defense, for example, employs 2.91 million people, and less than half of them, or 1.3 million, are active duty personnel.33 And unlike military functions such as fires or movement and maneuver of forces and equipment, many of the tasks related to military logistics and other financial, personnel, and health services are administered in noncombat settings.

While we discuss how the United States and its allies can work together on AI for military logistics and sustainment in both combat and noncombat settings, there is no doubt that the environment in question matters a great deal. From data to computational power to available talent, as well as considerations like privacy, safety, and security, implementing AI for military logistics and sustainment functions performed in controlled environments similar to commercial settings is a different endeavor from deploying AIenabled logistics and sustainment functions in contested and hostile environments. We take these differences into account where relevant, and acknowledge that even under the best of circumstances, there are still significant challenges for both the adoption of AI applications and multinational collaboration in this area.

Technologically attainable While not without its challenges, military logistics and sustainment tasks, especially those performed in noncombat settings, present a technologically attainable area for multinational collaboration in AI. Although much of the innovation in AI is occurring in the commercial sector, adopting and adapting commercial AI applications for military purposes is often impossible. Current AI technologies, and especially ML-based systems, tend to perform well in stable environments but struggle with uncertain and novel situations, and remain particularly vulnerable to adversarial attacks.

These vulnerabilities present an unacceptable level of risk in highstakes military settings, where the environment is uncertain and adversarial by definition. The consequences of mistakes and even system failure, however, are less severe when it comes to some military logistics and sustainment tasks which are administered and managed in noncombat settings, and constitute what some have called enterprise AI applications.

Advances in AI for logistics in commercial aviation, maritime shipping, and transportation sectors are therefore more applicable to certain military logistics and sustainment tasks performed in noncombat settings than for specialized military equipment like autonomous ground combat vehicles or armed drones. In particular, there may be opportunities to adopt and adapt commercial applications for the intelligent automation of tasks such as scheduling equipment maintenance and repairs, updating and issuing licenses, supply tracking and forecasting, and other processes that control the flow of logistics throughout the military organization.34 To reiterate, these are much more than cost cutting and efficiency increasing measures; improvements in these areas enable military readiness and effectiveness in combat.35

In addition to these opportunities to leverage AI-enabled technologies and tools available in the commercial sector in support of military logistics, there are also fewer barriers to inhouse innovation within defense organizations. Many of the AI applications relevant to logistics and sustainment can be developed and used in relatively well-controlled and benign environments in settings akin to commercial civilian enterprises. Under such conditions, resources like data and infrastructure, including storage, ETL pipelines, communication bandwidth, and compute can be made available to train ML models for various AI applications.36 Notably, the 2016 Defense Science Board Summer Study on Autonomy raised a similar point regarding logistics planning and execution as “a particularly good candidate for testing and experimentation (T&E) … because the behavior of logistic software can be evaluated against crisply known metrics.”37

Considering both the potential for leveraging developments from the private sector and lower barriers to in-house innovation, collaboration on AI for logistics and sustainment could also involve allies with more limited military-industrial capacities. Based on its fact-finding mission to Singapore, NATO’s Science and Technology Committee observed that “small and medium-sized Allies with smart scientists and engineers can play an outsized role in AI development and adoption.”38 This is a significant advantage, arguably unique to AI technologies, and especially timely considering that even the relatively wealthy U.S. allies are facing cuts to their defense budgets due to the economic fallout from the COVID-19 pandemic. Moreover, collaboration that includes input from small and medium-sized allies can strengthen interoperability, contribute to allied burden sharing, and buttress the long-term viability of U.S.-led defense partnerships.

This is not to say that adopting and developing, let alone collaborating on AI-enabled logistics will be an easy task for the U.S. military and allied defense organizations. The ML and deep learning algorithms behind commercial AI-enabled logistics are generally not optimized for military needs.39 And if the experience of the Department of Defense is any indication, there are multiple challenges with regards to the data needed to power AI applications—from lack of data to problems with traceability, access, and interoperability of data collected by different systems.40 Moreover, data security and privacy concerns as well as different legal frameworks for how personal data is collected, handled, processed, and stored remain a critical barrier to international collaboration. Lack of clarity surrounding how to implement the exemptions for research incorporated into the General Data Protection Regulation, for example, has stalled collaboration between the U.S. National Institutes of Health and some European counterparts.41

These and other technical barriers and privacy-related concerns are indeed significant. But developments in privacy-preserving ML techniques, including homomorphic encryption, secure multi-party computation, and federated learning offer opportunities for allies to share and pool data without compromising the privacy of individual users and organizations whose data is being used.42 The United States can also work with allies to develop technical standards and protocols for harmonizing data collection, formatting, storage, and archiving to ensure data security and integrity.43

Overall, the U.S. military and allied defense organizations will face nonnegligible technical barriers whether adapting commercial AI technologies or building AI-enabled systems and tools in-house. From a comparative standpoint, however, military logistics and sustainment applications that fall under the broader category of enterprise AI applications present “low hanging fruit” for the U.S. military (and presumably for other technologically advanced militaries).44 Moreover, international collaboration on AI-enabled military logistics and sustainment is likely more within reach than collaboration on AI integrated into weapons systems or applications that feed on sensitive data collected by proprietary weapons and sensor systems.45

Politically feasible With key U.S. allies like the United Kingdom, Germany, France, South Korea and Japan already pursuing efforts to leverage AI for military logistics and sustainment, collaboration in this area seems politically feasible. The integration of AI into weapons systems has raised ethical concerns and opposition in some communities across the United States and in allied countries. Yet by focusing collaboration on AI applications for military logistics and sustainment functions, the United States and its allies could potentially sidestep the contentious “killer robots” debate. Collaborative efforts to develop and apply AI tools to areas such as defense supply chain management, personnel management, and equipment maintenance can improve existing processes and functions, save costs and increase efficiencies in defense organizations. Multinational collaboration around this set of goals and applications is less likely to galvanize widespread grassroots opposition than programs on AI-enabled drones or autonomous ground combat vehicles.

Moreover, some of the United States’ closest allies are already investing in AI and ML technologies for logistics and sustainment. The United Kingdom’s Ministry of Defense’s (MOD) Autonomy Programme, for example, identifies defense resupply and logistics challenges through the Defense and Security Accelerator as one of its key activities.46 In 2019, MOD also allocated £66 million (about $83 million) to accelerate robotic projects for the British Army, including autonomous logistics vehicles supporting resupply missions in conflict zones.47 Notably, the UK’s Defense Science and Technology Laboratory and the U.S. Army Combat Capabilities Development Command’s Ground Vehicle Systems Center have been working together since 2016 on the Coalition Assured Autonomous Resupply project, prototyping semiautonomous logistics convoys, along with ground and aerial autonomous resupply systems, and demonstrating the interoperability of the two nations’ armies with autonomous driving technology.48

France’s military AI strategy also views “logistics and operational readiness” as one of the priority areas for the defense ministry, including a focus on predictive maintenance. 49 Notably, the strategy states that “mission performance and assisted maintenance applications, especially for cooperation with countries that have the same systems” as France pose no significant problems in terms of sharing classified data. And in addition to its key European partners, France is also open to collaboration with the United States given the similar approach to AI development. 50 Along similar lines, the German Army identifies AI for personnel and material management, including predictive maintenance, as one of the main areas for action on AI development.51

Japan and South Korea are also increasingly investing in military applications of AI, including for logistics and sustainment. South Korea’s National Strategy for Artificial Intelligence lists national defense as a key area for AI applications, including using AI to “quickly analyze and process large-scale defense data and develop and support common services such as medical care, logistics, and administration.”52 Meanwhile, Japan’s Acquisition, Technology and Logistics Agency (ATLA) has identified “logistical support technologies” in its medium- to long-term defense technology outlook back in 2016. More recently, ATLA has been working with private sector partners on research and development projects applying AI for defense logistics and “streamlining system maintenance work.”53

Efforts to advance collaboration on AI-enabled military logistics and sustainment will likely face some resistance. The aforementioned challenges related to data privacy are not merely technical in nature, but deeply political as well. Some European policymakers are pushing toward data sovereignty and less dependency on U.S. technology. Others are doubting whether the United States is willing to advance meaningful regulations over digital technologies and safeguards for data privacy.54 The question of a forum for collaboration remains a politically sensitive topic as well, even more so now in the aftermath of Brexit. 55

These challenges notwithstanding, the United States and its allies have shared interests and common policy objectives in ensuring the safe and responsible use of AI in alignment with democratic norms and principles. And with allies like the United Kingdom, France, Germany, South Korea, and Japan already promoting initiatives to leverage AI for military logistics and sustainment, this seems like a politically pragmatic area for collaboration.

Strategically critical The strategic environment in Europe and the Asia-Pacific region heightens the importance of coordinating national and multinational logistics, while collaboration on AI-enabled logistics can provide an operational advantage in multinational operations.

The U.S. military is a global force that must remain ahead of competitors and adversaries and be prepared for a broad range of contingencies and missions. Yet in multinational operations, the gap in military and technological capabilities between the United States and its allies and partners, and more specifically, significant discrepancies in allies’ logistic capabilities, can negatively impact survivability, interoperability, cohesion, and ultimately, mission success. Thus, for the United States and its allies, collaboration on logistics and sustainment in general, and on AI-enabled logistics and sustainment in particular, is important for several operational and strategic reasons.

Operationally speaking, logistic support during multinational military operations differs from unilateral operations. Nations have different national and military objectives, cultures, capabilities, and approaches to logistic support and functions. These differences impact how the United States military organizes, prepares, and eventually executes logistic support during multinational operations.56 Moreover, in multinational operations, nations share a collective responsibility for logistics in support of the mission. Thus, the logistic capabilities of each allied nation affect not only their ability to support their own forces but the operational-level support capabilities of the coalition as a whole.57

On a strategic level, the global threat landscape and U.S. security posture in Europe and the Asia-Pacific region elevate the significance of joint, streamlined logistics and comparable military endurance capabilities between the United States and its allies. In Europe, on NATO’s eastern flank, the Baltic states of Estonia and Latvia, (as well as potentially Lithuania) could be overrun by Russia’s superior military forces in a matter of days.58 Thus, in the event of a major conflict in the Baltic states, NATO would have to move thousands of troops and heavy military equipment from across Europe as well as from the United States very rapidly and efficiently to counter Russian aggression. Sound logistics—from the coordination and transfer of military cargo ships and private merchant vessels to the surge and movement of military equipment and supplies along Europe’s roads, rivers, and incompatible rail infrastructure—would prove essential to success. 59

Preventing China from becoming a regional hegemon in East Asia and strengthening the U.S.-led security architecture in the western Pacific is high on the list of U.S. strategic interests. Yet the U.S. military has no local shore bases from which to project power in the region, and its dependence on more distant bases in Guam, Japan, and South Korea, presents significant operational limitations. Moreover, U.S. air bases, aircraft carriers, surface vessels, ports, airfields, and logistics systems—those already in the region and those surge forces moving into the theater in the event of a crisis or a conflict—are currently vulnerable to Chinese air and missile attacks and cyberattacks.60 U.S. national security experts are well aware of these challenges and recognize the need to work with allies to protect shared security interests in these strategically important regions. For instance, the NSCAI’s interim report recommends assisting NATO in its adoption of AI and negotiating formal AI cooperation agreements with allies and partners like Australia, India, Japan, New Zealand, South Korea, and Vietnam.61 Moreover, the report explicitly recommends that U.S. alliances, primarily NATO, “explore pilot projects in low-risk areas such as for enterprise AI applications (logistics and sustainment) to derive lessons that would support broader application of AI systems for alliance efforts.”62

Along similar lines, in their assessment of U.S. competitiveness in the Indo-Pacific region, the Center for a New American Security recommends integrating logistics and sustainment considerations into the U.S. military strategy and operational concept development for China in order to ensure that the United States is able to project and sustain combat power in the Indo-Pacific region. 63 These efforts, however, could be strengthened by paying closer attention to the role AI/ML technologies could have in enabling more responsive logistics systems as well as in building the capacity of key partners in the region.

Certainly, when it comes to international collaboration in general, or collaborative AI projects related to military logistics and sustainment more specifically, disagreements and complications are inevitable. The past four years have seen more friction between NATO member states as well as between the United States and NATO. Rebuilding U.S. alliances is high on the Biden administration’s agenda. But restoring trust and good collaborative relationships takes time, effort, and resources. Moreover, NATO member states have very different military and technological capabilities which makes it difficult to implement alliance-wide initiatives. And while confronting China’s assertiveness is a top priority for the United States, many of the United States’ European and Asia-Pacific allies have economic and technological relationships with China. Their objectives vis-à-vis China on questions of geopolitics and technology are not necessarily aligned with those of the United States.

Nevertheless, the strategic and operational arguments in favor of working together on AI-enabled logistics and sustainment are quite powerful. Coordination on AI embedded in logistic systems can make for more efficient and streamlined movement of personnel and equipment, enable interoperability between systems and forces, and expedite the provision of medical services. Such improvements directly contribute to the readiness and endurance of allied military forces and their ability to deter and defeat adversaries if conflict erupts.

#### NATO and logistics are key---it’s uncontroversial and establishes standards necessary for broader cooperation---other organizations fail

Ulrike Esther Franke 21, senior policy fellow at the European Council on Foreign Relations (ECFR). She leads ECFR’s Technology and European Power initiative. Her areas of focus include German and European security and defence, the future of warfare, and the impact of new technologies such as drones and artificial intelligence on geopolitics and warfare. PhD in International Relations from the University of Oxford. Franke is a policy affiliate at the Governance of AI project at Oxford University’s Future of Humanity Institute. "Artificial divide: How Europe and America could clash over AI" – ECFR/367 2. January. <https://ecfr.eu/wp-content/uploads/Artificial-divide-How-Europe-and-America-could-clash-over-AI.pdf> //pipk

AI can enable applications in fields as diverse as health, robotics, defence, and agriculture. Where should the focus of potential transatlantic cooperation lie?

If Europe and the US agree to focus on AI ethics, then they should seek to develop common rules and guidelines that both sides can enforce in their jurisdictions. However, if they agree that their shared goal is to slow down other actors’ – particularly China’s – AI advances, they will need to engage in more targeted forms of cooperation. US researchers have proposed several specific initiatives for international cooperation, such as coordinating investment screening procedures, and establishing common export controls on supply chain components, to ensure China remains dependent on imports of AI chips. This would be in addition to the long line of measures already introduced by the US Department of Commerce. These include requirements for Chinese company Huawei to apply for licences to purchase semiconductors, a measure that aims to exert economic pressure and disrupt Chinese technology supply chains.

As noted, agreeing on shared goals and supporting measures will present some challenges. Beyond the specific themes of ethical AI and slowing Chinese progress in AI, however, there are other areas for transatlantic AI cooperation. Investing in these potentially less controversial areas may help create new platforms and lay important groundwork for greater cooperation. For example, the transatlantic allies should facilitate the exchange of knowledge and best practices on AI, and invest in mutually beneficial research, such as privacy-preserving machine learning.

Defence might also be a promising area for transatlantic cooperation, given the close military ties between the US and Europe through NATO. Military experts are raising concerns over how the introduction of AI onto the battlefield may hinder interoperability between allied forces, so defence could be a good realm in which to strengthen cooperation.

Militaries on both sides of the Atlantic are already investing in AI-enabled capabilities. In military affairs, as in the civilian realm, AI has a variety of uses. Military AI applications include autonomous vehicles and weapons; intelligence, surveillance, and reconnaissance; logistics (for example, the predictive maintenance of military systems such as vehicles and weapons); forecasting; and training (such as that in virtual reality simulations).

Some of these military capabilities – namely, lethal autonomous weapon systems, or “killer robots” – are among the most controversial uses of AI. The US and its European allies have adopted different positions on this issue in international debates such as those at the United Nations in Geneva, where lethal autonomous weapons have been under discussion since 2014. Transatlantic cooperation on lethal autonomous weapons, or other combat-related capabilities, does not, therefore, look promising.

However, military AI includes many non-controversial uses, such as ‘sustainment’, which encompasses logistics as well as support activities such as financial management, personnel services, and health care. AI helps make these services more efficient and cost-effective; for example, predictive maintenance helps in monitoring a system, such as an aircraft, and can do things such as use various sensory inputs and data analysis to predict when parts of a system will need to be replaced. Equally, AI can help improve logistics’ efficiency by, for instance, ensuring that supplies are delivered in appropriate quantities and at the right time. Transatlantic cooperation in this field is uncontroversial, but extremely useful – especially when carried out within NATO, as this could help bring allies closer together, establish joint procedures, and thereby ensure interoperability.

Which forum is best for fostering transatlantic AI cooperation? The US and most of its European allies already work together in a multitude of settings, with NATO foremost among them. Other international organisations and meetings – such as the G7, the G20, and the Five Eyes – bring together the US and some Europeans, as well as other actors. In addition, several new alliances and partnerships focused on technology or AI have been proposed or were already established over the last year: Europe and the US will need to choose the appropriate forum for AI cooperation based on its area of focus. Transatlantic cooperation on military AI might be best located within NATO. Members of the alliance have a long history of working together, and NATO already has dedicated units whose task is to ensure that all allies can cooperate and transform together. Given that military interoperability is vital to its functioning, NATO has no alternative but to address this issue, independent of other forums’ work. It would be advisable for NATO, and possibly the EU and its member states, to join the newly established, US-led AI partnership for defence. The current situation – in which the partnership includes only a few European countries and some of the United States’ other like-minded partners – is not constructive from a European viewpoint: Europeans should strive for Europe-wide harmonisation, not the creation of further differences. For cooperation on other areas of AI, such as sharing data or supporting research, other forums, including ad hoc alliances aimed at specific outcomes, may be the way forward. From a European standpoint, however, it would be advisable to try to include the EU as much as possible, so that European positions are not watered down or member states divided among themselves.

#### NATO has already signaled commitment to cooperation through the AI Strategy and Principles of Responsible Use---following through with experimentation to test specific capabilities signals commitment to ethical AI standards, provides effective evaluation for implementing the AI strategy effectively, and aligns with international law—spills over to international cooperation and discussions on AI and other emerging threats broadly---acting now is key

Zoe Stanley-Lockman & Edward Hunter Christie 21, Innovation Officer in the Emerging Security Challenges Division in NATO’s International Staff, and focuses particularly on Artificial Intelligence and Autonomy. owner and founder of AI Policy Consulting and served as lead consultant to NATO in the preparation of NATO’s AI Strategy. He was formerly Deputy Head of Innovation in NATO’s International Staff and the author of NATO’s Artificial Intelligence White Paper. "An Artificial Intelligence Strategy for NATO" October 25. <https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html> //pipk

Introduction

One does not have to look far to see how Artificial Intelligence (AI) – the ability of machines to perform tasks that typically require human intelligence – is transforming the international security environment in which NATO operates. Due to its cross-cutting nature, AI will pose a broad set of international security challenges, affecting both traditional military capabilities and the realm of hybrid threats, and will likewise provide new opportunities to respond to them. AI will have an impact on all of NATO’s core tasks of collective defence, crisis management, and cooperative security.

With new opportunities, risks, and threats to prosperity and security at stake, the promise and peril associated with this foundational technology are too vast for any single actor to manage alone. As a result, cooperation is inherently needed to equally mitigate international security risks, as well as to capitalise on the technology’s potential to transform enterprise functions, mission support, and operations.

The continued ability of the Alliance to deter and defend against any potential adversary and to respond effectively to emerging crises will hinge on its ability to maintain its technological edge. Militarily, futureproofing the comparative advantage of Allied forces will depend on a common policy basis and digital backbone to ensure interoperability and accordance with international law. With the fusion of human, information, and physical elements increasingly determining decisive advantage in the battlespace, interoperability becomes all the more essential. Further, as competitors and potential adversaries invest in AI for military purposes, ensuring that Allies develop common responses to ensure their collective security will only become more urgent.

With the formal adoption of the NATO AI Strategy, Allies have committed to the necessary cooperation and collaboration to meet these very challenges in both defence and security, naming NATO as the primary transatlantic forum. The aim of NATO’s AI Strategy is to accelerate AI adoption by enhancing key AI enablers and adapting policy, including by adopting Principles of Responsible Use for AI and by safeguarding against threats from malicious use of AI by state and non-state actors.

By acting collectively through NATO, Allied governments also ensure a continued focus on interoperability and the development of common standards. Overall, with innovation ecosystems implicating different actors and faster technology lifecycles than typically included in traditional capability development systems, the NATO AI Strategy is also a recognition that exploitation of AI will require new efforts to foster and leverage the Alliance’s innovation potential, including through new partnerships and mechanisms. Taken together, these efforts will in turn strengthen the Alliance’s ability to pursue cooperative security efforts and to engage with international partners and other international organisations on matters of international security.

Principles of Responsible Use

Adopting AI in the defence and security context also calls for effective and responsible governance, in line with the common values and international commitments of Allied nations. To that end, Allied governments have committed to Principles of Responsible Use as a key component of NATO’s AI Strategy.

Allies and NATO commit to ensuring that the AI applications they develop and consider for deployment will be in accordance with the following six principles:

Lawfulness: AI applications will be developed and used in accordance with national and international law, including international humanitarian law and human rights law, as applicable.

Responsibility and Accountability: AI applications will be developed and used with appropriate levels of judgment and care; clear human responsibility shall apply in order to ensure accountability.

Explainability and Traceability: AI applications will be appropriately understandable and transparent, including through the use of review methodologies, sources, and procedures. This includes verification, assessment and validation mechanisms at either a NATO and/or national level.

Reliability: AI applications will have explicit, well-defined use cases. The safety, security, and robustness of such capabilities will be subject to testing and assurance within those use cases across their entire life cycle, including through established NATO and/or national certification procedures.

Governability: AI applications will be developed and used according to their intended functions and will allow for: appropriate human-machine interaction; the ability to detect and avoid unintended consequences; and the ability to take steps, such as disengagement or deactivation of systems, when such systems demonstrate unintended behaviour.

Bias Mitigation: Proactive steps will be taken to minimise any unintended bias in the development and use of AI applications and in data sets.

Having agreed to adopt these mutually reinforcing principles, the task now turns to translating them into principled action. As such, NATO’s role in operationalising these principles will involve efforts that similarly tackle different aspects of the technology’s lifecycle. Building the principles of responsible use into the front end of AI development is important because, the later they are considered, the harder it may be to ensure they are upheld. Ensuring a full life-cycle approach also depends on multi-stakeholder engagement because responsibility is diffused amongst the policymakers, designers, developers, and testers, as well as operational end users that engage in AI development and use. For NATO, this is relevant because various entities play an active role in AI integration, and because the Alliance can encourage coherence with national AI developments.

For NATO, the common commitment to these principles has practical advantages as well, providing a coherent common basis for both NATO and Allies to design and develop AI applications while also supporting interoperability goals. As such, NATO can foster the necessary interlinkages between safety, security, responsible use, and interoperability. This can be seen across the principles. For instance, it is important to ensure that AI systems are adequately robust and reliable for their intended use, not only so that they can be expected to function in accordance with legal obligations, but also to mitigate the risks of the system’s defects or limitations being exploited by nefarious actors.

Putting Principles into Practice

These enduring principles are also foundational to the discussion and adoption of more detailed best practices and standards. Allies and NATO can leverage NATO’s consultative mechanisms and NATO’s specialised staff and facilities to work actively towards that goal. NATO’s own standardisation and certification efforts can also be bolstered by coherence with relevant international standard-setting bodies, including for civilian AI standards.

In addition to best practices and standards, these principles can also be operationalised via other mechanisms including review methodologies, risk and impact assessments, and security certification requirements like threat analysis frameworks and audits, among others. Further, NATO’s cooperative activities provide the basis to test, evaluate, validate, and verify (TEVV) AI-enabled capabilities in various different contexts. More specifically, NATO’s experience not only in operations, but also in trials, exercises, and experimentation provide several avenues in which Allies and NATO can test principles against intended use cases. This is further reinforced by NATO’s scientific and technical communities, which have worked on issues such as trust, human-machine and machine-machine interactions, and human-systems integration, among many others.

In addition to these existing activities, the implementation of the AI Strategy will also benefit from connections with NATO’s forthcoming Defence Innovation Accelerator for the North Atlantic (DIANA). Allied Test Centres affiliated with DIANA could be used to fulfil the aims set out in the definitions of the principles. In the future, use of these Test Centres can help ensure that AI adoption and integration are tested for robustness and resilience. For example, to ensure that AI is Traceable, Reliable and Bias-mitigating, Test Centres could synthesise how AI systems perform in different simulated environments and on different testing data, or provide independent validation and verification to assess compliance with standards that focus on responsible engineering practices.

Through the adoption of principles of responsible use, NATO and Allies are sending a deliberately public message to their domestic populations, to Allied forces, and to other states, reiterating the Alliance’s enduring values and commitments under international law. More than just an obligation, this democratic commitment is also a pre-condition for common policy bases among Allies – and for partnership with non-traditional innovators across the Alliance.

Accelerating principled and interoperable adoption

With the ethical aspects of adoption that the principles underscore, NATO has the chance to signal – and follow through on – responsibility at the core of its outreach efforts. This includes engagement with start-ups, innovative small and medium enterprises, and academic researchers that either have not considered working on defence and security solutions, or simply find the adoption pathways too slow or restrictive for their business models. In contrast to the development of traditional military platforms, AI integration entails fast refresh cycles and requires constant upgrading. This requires a change of mind-set for iterative, adaptive capability development, in contrast to sequential development cycles that take years to deliver small numbers of highly sophisticated platforms. With hostile state and non-state actors increasing their investments in Emerging and Disruptive Technologies including AI, this more flexible approach to adoption is all the more urgent. In this context, with its focus on TEVV and collaborative activities, the AI Strategy sets the framework for technological enablers to out-adapt competitors and adversaries. With more of a focus on agility and adaptation, NATO can make defence and security a more attractive sector for civilian innovators to partner with, while also allowing them to maintain other commercial opportunities. In doing so, efforts to bolster the transatlantic innovation ecosystem can also serve as a bulwark against undesirable foreign investment and technology transfers.

This work requires coordination across the NATO Enterprise. Indeed, several stakeholders across the NATO Enterprise are already involved in the development of AI-related use cases, concepts, and programmes. With the AI Strategy, these activities can gain coherence to ensure the proper connections exist between all innovation stakeholders, including operational end-users.

Moving Ahead

To be sure, the implementation of accelerated, principled, and interoperable AI adoption depends not just on technology, but equally on the talented and empowered people who drive the technological state-of-the-art and integration forward. NATO has also dedicated attention to other AI inputs, notably through the development of a NATO Data Exploitation Framework Policy. With actions to treat data as a strategic asset, develop analytical tools, and store and manage data in the appropriate infrastructure, the Data Exploitation Framework Policy sets the conditions for the AI Strategy’s success.

In addition to the interrelationships between data and AI, ensuring coherence between NATO’s efforts on AI and other Emerging and Disruptive Technologies such as autonomy, biotechnology, and quantum computing will be vital. As Allies and NATO seek to fulfil the aim of this AI Strategy, the linkages between responsible use, accelerated adoption, interoperability, and safeguarding against threats are critical. Indeed, these linkages will also apply to NATO’s follow-on work on other Emerging and Disruptive Technologies, including the development of principles of responsible use. More broadly, this entails further coherence between the work strands on these technologies, understanding that NATO’s future technological edge – and threats the Alliance will face – may depend on their convergence.

As such, not only does the NATO AI Strategy apply to this foundational technology, but it also sets the stage for NATO’s and Allies’ ambitions with regards to other Emerging and Disruptive Technologies. For each of them, the future strategic advantage that comes with NATO innovation efforts will derive from the connections between ethical leadership, iterative adoption, and integration that prizes flexibility, interoperability, and trust.

#### US-NATO cooperation is key to AI leadership---the US and Europe each have strengths, they just need a forum to effectively coordinate strategies to maximize return---diffusion and development of AI is inevitable, it’s only a question of maintaining the relative lead---no counterplan can solve all the internal links---process is either normal means, causes delays, or discourages necessary private investment

E.H. Christie 22, Senior Research Fellow, Finnish Institute of International Affairs, Arkadiankatu. Former liaison between the NATO Innovation Unit and the Commission’s staff. March 31. "Defence cooperation in artificial intelligence: Bridging the transatlantic gap for a stronger Europe" Wilfried Martens Centre for European Studies. European View, 1-9. <https://journals.sagepub.com/doi/pdf/10.1177/17816858221089372> //pipk

This article provides a brief overview of European and transatlantic defence cooperation in the area of artificial intelligence. As states race forward to achieve superiority in artificial intelligence, including its military applications, NATO allies and partner nations on both sides of the Atlantic have a strong incentive to cooperate closely and ensure the collective West can maintain its technological edge. However, large gaps remain between the US and the EU on certain key indicators. To ensure greater European performance and relevance, it is 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.

Artificial intelligence (AI) is the ability of machines to perform tasks that typically require human intelligence—for example, recognising patterns, learning from experience, drawing conclusions, making predictions or taking action—whether digitally or as the smart software behind autonomous physical systems (Reding and Eaton 2020, 14).

The range of potential military applications is at least as vast as the range of tasks that require human cognition, for example analysing and classifying visual data, organising logistics, operating support vehicles, or tracking and engaging hostile targets (Christie 2021b, 84). States are racing to achieve superiority in the AI domain (Lin-Greenberg 2020). Furthermore, like other digital technologies, AI diffuses rapidly and cheaply across areas of human activity and across borders. Nevertheless, as with other technological transformations, states with greater resources and levels of effort, and better policies, will reap the benefits of technology adoption more rapidly than others.

In an alliance context, matters pertaining to cooperation and interoperability take centre stage. The good news is that Europeans are not starting from scratch. European states that are members of NATO can rely on decades of experience with the Alliance’s mechanisms of consultation and collaboration. In addition, European states that are members of the EU can pursue collaborative activities through the European Defence Agency (EDA). Furthermore, EU funding is available through the European Defence Fund for defence research and capability-development activities.

At NATO the key processes address, most notably, the areas of defence research, military transformation, capability development, military–technical standardisation, and defence planning and capability targets. For these areas of work, formal consultative mechanisms—committees in which each Ally has a voice—include the Science and Technology Board, the Military Committee, the Conference of National Armaments Directors, the NATO Standardisation Board, and the Defence Policy and Planning Committee. Each of these committees relies on support staffs and structures. Of particular interest when considering AI are the Science and Technology Organisation, which has several facilities and is led by the Office of the Chief Scientist at NATO Headquarters; and, Allied Command Transformation. The latter, including its Innovation Hub, plays a particularly central role in driving innovation and force transformation for the Alliance. In addition, two staff units created in 2019 are of particular importance, namely the Innovation Unit and the Data Policy Unit, both of which are within the Emerging Security Challenges Division of the NATO International Staff. The Innovation Unit provides thought leadership and initiatives to accelerate technology adoption, while the Data Policy Unit provides policy thought leadership on how to treat data as a strategic resource. The Innovation Unit designs new initiatives for the promotion and financing of defence-related innovation. A notable achievement in this area was the creation of the NATO Innovation Fund (NATO 2021).

In the EU context, the EDA plays a central role in several areas of work. Among other activities, the EDA supports defence research cooperation, defence standardisation and pooled procurement programmes, while also contributing to the EU’s Capability Development Plan and Coordinated Annual Review on Defence (Fiott 2018, 287). Most of the EDA’s functions are broadly analogous to ones that exist at NATO. Of particular interest is the intention to create a new Defence Innovation Hub within the EDA, as announced in the EU’s November 2021 draft Strategic Compass (European External Action Service 2021, 23).

Before proceeding, it is worth spelling out the extent to which European security is dependent on NATO and in particular on the US. Of the EU’s 27 member states, 21 are members of NATO. These countries account for about 93% of the population1 of the EU. Within NATO, those Allies that are also EU members only account for about 20% of total defence expenditure across the Alliance, while the US alone accounts for about 70% of the same total.2 Beyond these aggregate indicators, it is furthermore the case that the US is considerably ahead of the EU in terms of practical adoption of AI. For illustration, in 2020 US private-sector investment in AI was around $23.6 billion, but was only $2 billion in the EU, implying a ratio of 12 to 1 in favour of the US (Zhang et al. 2021, 96). Scientific output indicators offer a more nuanced picture. In 2019, the EU accounted for 16.4% of the world’s peer-reviewed AI publications, ahead of the US with 14.6%, while China occupied the top spot with 22.4% (Zhang et al. 2021, 20). On the other hand, if one measures research output in terms of publications on the Arxiv database, the US is ahead of the EU (Zhang et al. 2021, 33) by a ratio of almost two to one, which is nonetheless much less than the large gap in private investment mentioned above. That the EU performs similarly to the US in terms of scientific research, but far less well in terms of investment and commercialisation of new digital technologies, is an old problem which has proven very difficult to address, whether at national or EU level (Baroudy et al. 2020).

In the following sections, I offer reflections on three challenge areas for European and Allied defence institutions: interoperability challenges, international security challenges and investment challenges. These three challenges are effectively interdependent. While interoperability is a permanent goal in an alliance context, be it NATO or the EU, it is particularly salient in cases of rapid technological change, such as with AI, as there is a need for a higher tempo across areas of activity. Heightened international security challenges likewise increase the need for urgency to ensure that Western nations do not fall behind potential adversaries. Investment, in turn, is the engine for rapid change, enabling the dynamic adoption of new technologies, relevant capability-development activities and other adaptations along the value chain of military activities. Overall, my central argument is that the confluence of rapid technological change and heightened international security challenges requires a higher pace of change and adaptation that can only succeed if serious investments are made on both sides of the Atlantic.

Interoperability challenges

Interoperability can be defined as ‘the ability of systems, units or forces to provide services to, and accept services from other systems, units or forces and the use the services so exchanged to enable them to operate effectively together’ (Dufour 2018, 1).

The first general challenge to interoperability is the overall gap between the US and Europe in terms of total defence investment, as well as in terms of civilian technological attainment with respect to AI and related technologies. There is no single solution to this problem, which is much broader in scope than traditional military–technical standards, such as those pursued in the NATO context through existing mechanisms. For this broad challenge, overall policy decisions relating to national investment choices and technology policy coordination between the two sides of the Atlantic are of particular importance. Further discussion of this follows in the sections on investment challenges and international security challenges.

A second challenge to interoperability is that, as far as digital technologies are concerned, the civilian sector of the economy, on both sides of the Atlantic, is more advanced, more dynamic and also not especially oriented towards meeting military needs. For decades, the military sector has represented only a very small share of the total sales volume of the computing and semiconductor industries. The same pattern is repeating itself currently with AI. This stands in great contrast to narrower dual-use technologies, for example aerospace, where the military sector remains inherently important. With digital technologies, defence institutions are under much more pressure to either adapt to civilian industry products and standards or to pay a significant premium to suppliers to secure military-grade equipment and software.

A third challenge to interoperability lies in how AI is implemented in practice. To set up a bespoke machine-learning algorithm in a given data environment, best practice in the software industry is to pursue some variant of ‘agile’ development. This involves a very different product-development cycle, essentially proceeding with multiple rapid iterations of an imperfect product that is released in preliminary versions and later revised—like software products released in various ‘beta versions’—with upgrades developed over time. This contrasts greatly with the traditional production of major military platforms, which puts a premium on strict quality control and compliance with requirements at every development step—an approach referred to in the software industry as ‘waterfall’ development (Christie 2021b, 87). Agile product development may pose challenges to interoperability. Unless very tight standards are applied, there is a considerable risk of divergences in how different national institutions go about solving a particular AI or data analytics problem.

With large traditional military platforms there are long time frames during which states can take coordination steps, either by purchasing the same platforms, or by building consensus in terms of requirements and standards. However, when a comparatively small team works dynamically to generate an algorithmic solution to a particular problem in a matter of weeks or months, traditional coordination through existing consultation mechanisms may pose risks to the speed advantage inherent to agile development. Conversely, once a solution has been developed, its adoption in somewhat different environments may be challenging for a range of technical reasons. None of these issues is insurmountable, but they do pose, in a new light, classical trade-offs between the benefits of inventiveness and dynamism, on the one hand, and those of imposing constraints through standards and other harmonising measures to ensure that new products can be broadly used and shared on the other. In the case of AI, a typical observation is that there are many excellent prototypes and pilot projects in numerous defence institutions, but there are also serious outstanding challenges in terms of scaling up to enterprise-wide solutions, let alone Alliance-wide solutions.

Finally, the question of ethical AI—or responsible AI—generates considerable attention on the part of governments and civil society. In response, NATO sought to establish a consensus on certain essential principles, referred to as Principles of Responsible Use, which build on emerging national commitments. These principles were endorsed by Allied governments in October 2021 (Stanley-Lockman and Christie 2021).

International security challenges

Both EU nations and the US are exposed to the same global environment and to similar strategic concerns, at the confluence of rapid technological change and global power shifts. Starting from around 2018, policy discourse in the US became particularly focused on fears of being overtaken by China technologically and militarily. A good illustration of these fears is a 2020 statement by the Director of the Federal Bureau of Investigation, who accused the Chinese government of ‘fighting a generational fight to surpass our country in economic and technological leadership’ and of ‘taking an all-tools and all-sectors approach . . . that demands our own all-tools and all-sectors approach in response’ (Wray 2020).

For military AI, China poses the greatest challenge to Western nations (Kania 2019). However, Russia is also actively pursuing such capabilities (Zysk 2021; Engvall 2021), including through espionage, for example against the Netherlands (AIVD 2020) and France (Follorou 2021).

Nations on both sides of the Atlantic have recognised the rising challenge of Chinese and Russian government-sponsored industrial espionage aimed at the illegitimate acquisition of cutting-edge Western technologies. And both the US and the EU have adopted strengthened legislation in several key areas, including on the protection of trade secrets, on export controls for dual-use items and on the screening of foreign direct investment (Christie 2021a). Another relevant area of work is measures to better protect the university and research sector from espionage. A new toolkit of recommendations now exists at EU level (European Commission 2022).

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 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 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.

## NATO Advantage

### 2AC---AI Coop Key to NATO

#### AI cooperation key to NATO effectiveness

Erik Lin-Greenberg 20, postdoctoral fellow at the University of Pennsylvania’s Perry World House. Texas National Security Review, Vol 3, Iss 2. Spring. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making" <https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/> //pipk

Second, incorporating AI-enabled capabilities into alliance planning exercises and wargames will help prepare policymakers and commanders to better employ AI.132 Wargames, for instance, might ask leaders to employ AI-enabled capabilities or respond to a rival’s use of AI-enabled weapons. These events allow leaders to test and refine institutional processes in a low-risk environment, while also socializing practitioners to the potential uses, limitations, and risks of AI-enabled warfare.

Conclusion

As additional funding and research drive increases in the effectiveness and reliability of AI, the military use of AI technologies will likely expand. And as more states integrate AI into their armed forces, the United States will find itself working with allies to build and exercise AI capabilities that are interoperable and support alliance decision-making processes. Failure to cooperate early and often on the development and use of AI may leave allies ill-prepared for operations in an era in which AI is an increasingly common fixture in the arsenals of both friends and foes.133

Alliances face two broad sets of challenges when integrating AI into operations. First, AI complicates alliance operations. The resource and data requirements needed to build and maintain AI systems pose obstacles to burden-sharing and interoperability. Adversaries can also use AI to launch military deception campaigns that complicate operational coordination. Second, AI can significantly strain alliance decision-making. New AI technologies promise to increase the speed with which allies and adversaries conduct operations, decreasing the time partners have to debate potential courses of action. Decision-making can also be disrupted if adversaries use AI to generate misinformation that can degrade trust among allies. To overcome these challenges, allies will need to establish multinational agreements and standardization guidelines that help ensure data is structured in ways that promote interoperability, while technical measures will help preserve data privacy, allow for data sharing, and minimize the consequences of AI use on the part of adversaries.

Whether and how states grapple with these challenges will shape the conduct of multinational operations and has implications for alliance politics and the global balance of power. Alliances that effectively integrate AI technology will be better positioned to counter threats, while those that allow AI to stymie decision-making and operations may find themselves disadvantaged on the battlefield. Within alliances, member states that quickly master the integration of AI into their militaries may gain significant influence, even if they are less powerful than other alliance partners in conventional terms. Because of their AI know-how, these states may play a dominant role in developing the norms, standards, and doctrine for AI use and help set an alliance’s AI strategy. In a similar vein, Estonia leveraged its cyber warfare expertise to bolster its position in NATO. Despite being territorially small and weak in conventional military terms, Estonia’s specialized expertise allowed it to play a leading role in shaping NATO’s cyber doctrine.134 A state’s successful development of AI can therefore increase its voice and sway within complex multinational institutions.

This article represents a first step in understanding how the burgeoning development of AI technologies will affect alliances, and offers a framework for future hypothesis testing. Future work might more systematically explore the ways in which AI-enabled systems influence multinational military decision-making and operations. For instance, do national security decision-makers trust information provided by AI technologies more or less than information delivered by non-AI enabled sources? Under what conditions are decision-makers more or less likely to believe this information? Are military leaders from certain states more willing than those from other states to rely on AI technologies? If so, what drives this variation? Scholars might also try to identify the types of technical or institutional solutions that best promote AI interoperability. Do alliance decision-makers see formal agreements or technical solutions as a more effective means of ensuring data sharing? Scholars can explore these questions using a variety of methodological approaches including experimental research involving alliance decision-makers or in-depth case studies informed by interviews of senior policymakers.

Researchers might also consider the effects of AI on alliances in areas beyond decision-making and interoperability. For example, how does the use of AI affect strategic stability, nuclear deterrence, and alliance reassurance? Does the increased tempo of AI-enabled warfare make it harder or easier for states to deter rivals and reassure allies? Studies that address these questions would not only expand our scholarly understanding of the relationship between emerging technology and international security, but would help policymakers design better processes and institutions for a security environment in which AI use is becoming widespread.

As AI becomes increasingly common in military arsenals around the world, it is crucial for states to understand the potential challenges AI poses to multinational operations and work to overcome them. To prepare for warfare at machine speed, alliances should develop policies and practices that streamline data sharing and decision-making, and take procedural and technical measures to bolster their defenses against AI-equipped rivals.

#### Tech gaps bad for interoperability---ensuring smaller allies can contribute is key

Simona R. Soare 21, was a Senior Associate Analyst at EUISS from 2019 to end May 2021. Her research focused on United States security policy, transatlantic security and EU-NATO relations. Prior to joining EUISS, Simona served as advisor to the Vice-President of the European Parliament (2015-2019) and as an analyst with the Romanian Ministry of Defence, working on transatlantic and European security. She has also been a research associate with the Institut d’Études Européennes (IEE) at Université Saint Louis-Bruxelles. Simona holds a PhD in Political Science from the National School for Political and Administrative Studies in Bucharest where she lectured on international security (2008-2015). She is the recipient of a U.S. Department of State fellowship on U.S. Grand Strategy and has published extensively on American and transatlantic security. "Innovation as Adaptation: NATO and Emerging Technologies" June 11. <https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies> //pipk

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.

### 2AC---AI key to NATO---Burden-Sharing Conflicts

#### AI gaps in NATO create burden-sharing conflicts

Erik Lin-Greenberg 20, postdoctoral fellow at the University of Pennsylvania’s Perry World House. Texas National Security Review, Vol 3, Iss 2. Spring. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making" <https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/> //pipk

The existence of “AI haves” and “have-nots” within an alliance can complicate burden-sharing — a central tenet of military alliances. On one hand, states with robust AI capabilities can specialize their contributions to alliance operations and focus on providing AI-related capabilities. If, however, AI applications become a necessity for warfighting in the future, states that lack AI capabilities may be less able to contribute to alliance operations. States better equipped with AI capabilities may subsequently be forced to take on a greater share of work, generating both political and operational challenges. Politically, “AI haves” may complain that “AI have-nots” are not adequately contributing to a mission, straining relations between allies. Operationally, capability gaps can hamper an alliance’s ability to deploy forces or achieve military objectives. During the NATO-led air war over Kosovo in 1999, for instance, many NATO members possessed limited numbers of precision-guided munitions in their arsenals and often lacked the training to employ them, curtailing their ability to contribute to operations.65 As a result, responsibility for carrying out the air campaign fell to a small number of allies. In a larger conflict, burden-sharing might be critical to sustaining operations or securing battlefield victories.

### 2AC---AI key to NATO---Interoperability

#### Interoperability collapsing---AI integration is key

Martin Dufour 18, Colonel in the Canadian Army, working with NATO. This Policy Brief is a revised version of a paper that was awarded the Eisenhower Prize for the best Individual Paper of NDC Senior Course 132. NATO Defense College, Research Division. NDC Policy Brief, No. 6. December. "Will artificial intelligence challenge NATO interoperability?" //pipk

At the operational and strategic levels, the adoption of artificial intelligence-enabled autonomous systems connecting sensors, battle management, command and control systems, as well as defensive and offensive assets in a network of learning, adaptive systems will enable “a form of algorithmic warfare and machine learning approach to targeting”10 which will compress the decision-action cycle to such an extent that countries not connected to the system will be unable to keep up.

The 2017 report Future War NATO argues that the “technologically-driven US military strategy is advancing so fast compared to European allies that, sooner rather than later, all-important NATO military interoperability might well become a thing of the past”.11 This echoed a 2016 report from the Armament Industry European Research Group, which concluded that “a further boost in US defence technology could promote a wider US-Europe gap and the emergence of a two-tier alliance”.12 It was furthermore observed that the USD3.6 billion invested in Third Offset Strategy technologies in 2017, while representing only 5 percent of the overall US military research and development budget corresponded “to more than 40 percent of the overall EU-European R&D budgets”.13

Beyond interoperability, a profound technological mismatch between allies could also erode the political and military cohesion of the Alliance by creating resentment between countries that bear a greater share of the burden as a result, and those that do not.

While challenges exist, artificial intelligence need not erode NATO cohesion. It is however imperative that countries begin to think seriously about the future impact of artificial intelligence, and how to effectively start adopting the technology. An exploratory look at the development landscape for artifi cial intelligence and autonomous technologies reveals that most of the innovations in the fi eld occur outside the military-industrial complex. The GAFAs (Google, Amazon, Facebook, Apple) have steadily invested over the years to develop commercial applications for artifi cial intelligence, and one can fi nd many other startup companies throughout the world. The data company CB Insights’ second annual AI 100 list identifi ed the 100 most promising artifi cial intelligence startups, noting that they came from nine different countries, including many from smaller nations which “in aggregate... have raised USD11.7 billion in equity funding across 367 deals”.14 NATO states should therefore strive to develop partnerships with such companies, identify promising applications, and start implementing them at once in their defence framework to act as agent of change.

It is also interesting to note that when it comes to successfully leveraging emerging technologies, the business model is often more important than the capability. One only needs consider the success of companies such as Uber and AirBnB, giants in their respective fi elds, but which do not actually own any physical assets. Smaller NATO nations should therefore reconsider their business model and identify niche domains such as cyberwarfare, early threat detection or predictive analysis. They could then leverage partnerships with promising companies to develop those capabilities to obtain a competitive advantage allowing them to remain relevant in times of confl ict. These capabilities could offset complex hardware solutions and allow smaller nations to continue sharing the burden of military opera tions. This is the point made in a 2017 study titled Artifi cial Intelligence and the Future of Defence, according to which given its “algorithmic and non-defence specifi c essence…[artifi cial intelligence] is easier to jump in than is the case for many industrial-kinetic technologies [such as] building a sixth-generation jet fi ghter”.15 As such smaller, nimble nations have an opportunity to redefi ne how they do military development, and harness this key disruptive technology to start fi lling the growing capability gap between NATO countries.

Overcoming the interoperability gap It is evident that of the emerging disruptive technologies, none is likely to have as signifi cant an impact on warfare as that of artifi cial intelligence. The effect of artifi cial intelligence is already being felt in numerous fi elds, and its further development and combination with other technologies will compound this, allowing the development of advanced autonomous systems. While the latter holds the promise of creating new classes of weapons with great military potential, disproportional growth among the various NATO allies could lead to complex interoperability problems, further widening the existing interoperability gap between member nations.

Over the next two decades Alliance members will be increasingly challenged by the rapid evolution of artifi cial intelligence and risk becoming unable to operate together should the asymmetric adoption of emerging technologies not be carefully managed. It is therefore paramount that countries begin preparing for the future impact of artifi cial intelligence in the military realm, and start adopting the technology in niche areas to ensure they do not fall too far behind.

#### Interoperability key to NATO---successful integration of AI is key

Martin Dufour 18, Colonel in the Canadian Army, working with NATO. This Policy Brief is a revised version of a paper that was awarded the Eisenhower Prize for the best Individual Paper of NDC Senior Course 132. NATO Defense College, Research Division. NDC Policy Brief, No. 6. December. "Will artificial intelligence challenge NATO interoperability?" //pipk

NATO has arguably been the most successful alliance of its kind, and much of this success can be attributed to its cohesion in the face of various threats. At the heart of this cohesion lie two important notions: burden sharing between members; and interoperability. The Alliance’s cohesion however has increasingly come under pressure over the last two decades, and there are growing challenges with the level of interoperability between member countries. While numerous technical and political factors influence interoperability, the emergence of disruptive technologies such as genetic engineering, nanotechnology, additive manufacturing and robotics, are likely to make this challenge more acute in the next two decades.

Of the many technologies rapidly emerging, none is likely to have as significant an impact as that of artificial intelligence, which combines with other technologies and multiply their effect by allowing the development of advanced autonomous systems. And while the latter holds the promise of developing new classes of weapons with great military potential, its asymmetrical adoption among the various NATO allies could also lead to significant interoperability problems.

What interoperability means Cohesion, often mentioned as the Alliance’s center of gravity, lies at the heart of NATO’s success. Underwriting this cohesion is the ability of member states to share the burden of producing military capabilities to service the whole, and the burden of conducting operational missions. To do this successfully, members have to be able to undertake military actions in concert with each other in a fully coordinated, and as much as possible integrated manner. This is referred to as interoperability, defined as “the ability of systems, units or forces to provide services to, and accept services from other systems, units or forces and to the use the services so exchanged to enable them to operate effectively together”.1

This definition implies that there are several layers to interoperability which need to be addressed to ensure forces are able to operate together effectively in a military context. These include technical features permitting systems to physically connect to one another and exchange information; and the alignment of procedures and processes to allow military personnel to function within the same space and achieve common goals without fratricide. It also implies that this takes place at various levels of operation, from tactical to strategic. A high level of interoperability allows allies to effectively exchange intelligence and information, cooperatively plan complex military operations, and conduct integrated missions with fully exchangeable force packages.

NATO interoperability challenges Historically NATO has had the tendency to focus on procedural and technical interoperability between systems. To do so, it has employed a standards-based approach and developed hundreds of Standardization Agreements (STANAGs) which provide member states agreed-upon processes, procedures and platform compliance specifications rather than stipulating what to build and how. While this approach has allowed member states to equip themselves but still successfully train and operate together for decades, the last 25 years has witnessed a growing rift in the military capabilities of different nations.

Rapid technological evolution and the increasing cost and complexity of contemporary military systems have made it progressively more difficult for several countries to keep pace with the systems of the bigger allies. For instance, some countries have invested heavily in advanced systems allowing them to collect and process intelligence, designate targets and strike them at will with standoff, precision-guided weapons, day and night in any weather conditions. The level of investment necessary to acquire such capabilities, as well as various politico-strategic concerns such as the protection of a country’s military-industrial base and resultant unwillingness to sell or transfer advanced technologies, have prevented other allies from remaining current with some of these innovations. These allies therefore lack the ability to gainfully partake in certain military operations and equally share the burden with other members of the Alliance.

The growing capability gap between NATO member nations was explored in a 2000 RAND Corporation study titled Interoperability: a continuing challenge in coalition air operations, which considered 40 contemporary coalition operations and concluded that there was a “growing divergence between US and NATO allies’ air forces in all-weather precision-strike capabilities to minimize collateral damage and employment of standoff weapons”.2 Using a specific example to highlight this point, the authors stated that “Allied contributions to recent strike operations in the Balkans have been limited because the allies lack sufficient precision-guided weapons that can be delivered day or night in any weather conditions”.3 While numerous countries have since taken steps to acquire precision-guided weapons, the US has continued to improve its capabilities, moving even further away from most allies during that same period. The 14 April 2018 strikes on Syrian chemical weapons sites is a recent example of this situation where, setting political considerations aside, only three countries (US, UK and France) were realistically in possession of the required standoff attack missiles capable of reaching targets deep inside Syria with precision, without putting the pilots and aircraft at undue risk from Syrian air defence systems. The same study also found that this growing interoperability gap also exists with other capabilities such as command and control systems, battle management systems, as well as information exchange and security. Most importantly, this problem has not gone away.4 The ability to gather, process and disseminate accurate intelligence to support effective decisions-making faster than the enemy’s ability to do so (the so called decision-action cycle) has always been the hallmark of effective military operations. In an age when most systems are interconnected, with proliferation of sensors and data repositories, information superiority is rapidly becoming a decisive factor for mission success. Therefore the ability of allies to rapidly share intelligence in a secure manner at the operational and strategic levels, and leverage this intelligence to make sound, common decisions is bound to become a determinant factor in who can participate in a mission in the future.

#### Intra NATO AI gap decks interoperability---cooperation through NATO is key

Matej Tonin 19, current Slovenian Minister of Defense, was an active member of the NATO PA from 2012 to 2020. He served as rapporteur and Chairperson of the Assembly's Sub-Committee on Technology Trends and Security and as Deputy Head of the Slovenian delegation to the NATO PA. "ARTIFICIAL INTELLIGENCE: IMPLICATIONS FOR NATO’S ARMED FORCES" Report from the Sub-Committee on Technology Trends and Security. October 13. <https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf> //pipk

63. Second, the defence technology gap between Allies must remain small enough to be bridged by interoperability. The large diversity of Allies is ultimately a primary source of NATO’s strength, but it also means that large differences exist in defence capabilities. There is a danger that the significant investment in AI in leading Allied nations could lead to substantial interoperability problems and a loss of NATO’s overall military effectiveness in the future. However, the good news is that AI efforts do not need to be capital intensive, as the Committee witnessed during its fact-finding visit to Singapore in May 2019. Small- and medium-sized Allies with smart scientists and engineers can play an outsized role in AI development and adoption if they so choose. This could indeed be a very effective contribution to Allied burden sharing from the smaller Allied nations. To increase interoperability, cooperation through NATO’ structures has a large role to play. Interoperability should be at the heart of AI efforts carried out by the STO, ACT, the NCI Agency, NIAG, and others. Allies leading in the S&T sector should encourage open architecture standards and regulations for technology sharing and transfer among Allies in order to narrow the technology gap, in line with all national obligations and the sensitive nature of technologies

64. Allied armed forces alone will not be able to solve the AI-specific challenges laid out in this report, including the ethical and legal questions. This will need a much broader push across the entire AI ecosystem. However, governments, NATO, and the EU can and must play a critical role in overcoming the investment, innovation, and workforce challenges of adopting AI. Just as national governments across the Alliance are rising to the challenge of AI, so should their armed forces. They should move beyond scanning the horizon and, instead, invest in real research, experimentation, development, and adoption efforts. It should be underlined that all dual-use and military AI efforts should, however, tackle all ethical, legal, and social questions right from the beginning, including privacy considerations and the definition of appropriate human involvement in decisions about the use of force. Allies should consider examining whether an ethics code of conduct could put the adoption of AI in the armed forces on a more stable foundation. At a strategic level, Allies must also address the geopolitical challenges, including the ones arising from Chinese and Russian investments in military AI systems. As this report has shown, Russia and China see AI as critical to future military power and invest heavily into AI-enabled military systems. For its part, the NATO PA Science and Technology Committee will continue to monitor AI developments in the defence sector through fact-finding visits and expert testimony.

### 2AC---NATO AI key to Deterrence

#### AI key to effective NATO deterrence versus Russia and China

Simona R. Soare 21, was a Senior Associate Analyst at EUISS from 2019 to end May 2021. Her research focused on United States security policy, transatlantic security and EU-NATO relations. Prior to joining EUISS, Simona served as advisor to the Vice-President of the European Parliament (2015-2019) and as an analyst with the Romanian Ministry of Defence, working on transatlantic and European security. She has also been a research associate with the Institut d’Études Européennes (IEE) at Université Saint Louis-Bruxelles. Simona holds a PhD in Political Science from the National School for Political and Administrative Studies in Bucharest where she lectured on international security (2008-2015). She is the recipient of a U.S. Department of State fellowship on U.S. Grand Strategy and has published extensively on American and transatlantic security. "Innovation as Adaptation: NATO and Emerging Technologies" June 11. <https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies> //pipk

Throughout NATO’s history, defense innovation has been critical to its technological edge and its deterrence and defense posture against multiple threats. The unprecedented progress in emerging and disruptive technologies (EDTs) offers the prospect and challenge of transformative defense innovation for allied armed forces and societies at large. Technological progress in artificial intelligence (AI) and machine learning, advanced robotics, biotechnologies and human enhancement, quantum technologies, big-data analytics, and fifth-generation telecommunication systems, as well as growing autonomy in the critical functions of military systems, promise to change how wars are fought, how fast, where, and by whom. These technologies enable new forms of military presence, coercive action, and power projection in and across old and new domains (for example, cyberspace and outer space) and below and above the conventional threshold of armed conflict.

However, NATO and the transatlantic allies are neither the only nor the most agile actors investing in emerging and disruptive technologies. China and Russia already invest substantially in and have accelerated their adoption of these technologies in military applications. To maintain its strategic advantage against China and Russia, NATO needs to become an agent of innovation and be more agile and strategic in supporting allies to jointly exploit new technologies for deterrence, defense, and resilience purposes. NATO has prioritized EDTs and signaled it has joined “the technological adoption race” against China and Russia.1 Much work remains to be done. Allies remain divided on the ethical and legal specifics of the military use of EDTs and by their national-industrial preferences. Technological capacity across the alliance also varies significantly and, as always, funding is in short supply. Concrete decisions on how to consolidate innovation in EDTs, a critical task for NATO’s mission and future adaptation, are expected at this month’s Brussels summit. Specifically, allies will respond to calls for a “strategic surge” in EDTs2 innovation by establishing a Defense Innovation Accelerator, an opt-in instrument funded through dedicated national contributions, which NATO hopes will incentivize innovation and transatlantic cooperation on emerging technologies.3

#### Solves multipolarity and deterrence

Simona R. Soare 21, was a Senior Associate Analyst at EUISS from 2019 to end May 2021. Her research focused on United States security policy, transatlantic security and EU-NATO relations. Prior to joining EUISS, Simona served as advisor to the Vice-President of the European Parliament (2015-2019) and as an analyst with the Romanian Ministry of Defence, working on transatlantic and European security. She has also been a research associate with the Institut d’Études Européennes (IEE) at Université Saint Louis-Bruxelles. Simona holds a PhD in Political Science from the National School for Political and Administrative Studies in Bucharest where she lectured on international security (2008-2015). She is the recipient of a U.S. Department of State fellowship on U.S. Grand Strategy and has published extensively on American and transatlantic security. "Innovation as Adaptation: NATO and Emerging Technologies" June 11. <https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies> //pipk

Conclusion

Long-term great-power competition has returned and it has a strong technological dimension. The time when NATO had the luxury to adapt at its own pace to a changing strategic environment is over. To survive and remain relevant in a multipolar world of rapidly evolving security risks and threats, and to compete successfully against Russia and China, NATO needs a new framework centered on innovation as adaptation. The alliance’s ongoing efforts in EDTs and the new NATO Strategic Concept are timely opportunities to start on this new path. A focus on inclusive innovation in NATO could increase adaptability and competitiveness in the long-term, help to disrupt, deter or defeat adversarial subversive actions, mitigate transnational threats and, more importantly, maintain solidarity and the principle of indivisible security among the allies.

### 2AC---AI Deters China

#### Effective and coordinated AI is key to credible deterrence against China

E.H. Christie 21, Senior Research Fellow, Finnish Institute of International Affairs, Arkadiankatu. Former liaison between the NATO Innovation Unit and the Commission’s staff. "Economics and Technology: Emerging New Threats [Speech transcript]." AI Policy Blog. ​ November 9. <https://www.aipolicyconsulting.com/economics-and-technology-new-threats> //pipk

We live in a world of Great Power competition.

Long gone are the days of simple, US- and EU-led globalisation, in which we could behave as if power politics didn’t exist.

The global strategic picture is probably well known to you all but let me lay it out briefly.

Two major security challenges take up a lot of bandwidth today, notably in the United States but also at NATO, across Europe, and really across the Western world. And I will address both. They are the following:

1/ The Rise of China

2/ and the rise of New Technologies, notably Artificial Intelligence

These two major transformative trends are already affecting everything we do, in the private sector, in public policy generally, and in national security and defence policy.

China’s economy, if one measures it at Purchasing Power Parities, is already 15% larger than that of the United States. And we should expect China to overtake America also in terms of current exchange rates, perhaps by 2035.

A world in which neither the United States nor the European Union are the biggest economy, or the biggest market, that is very new. It is radically new. During the Cold War, the Western Alliance faced a formidable enemy in the shape of the Soviet Union. But the Soviet Union never came close to overtaking America economically. At the very highest point and using the same type of conversion I used earlier, it may be that the USSR was two thirds of the US economy in equivalent material terms, and that was in the mid 1960s, and it didn’t last. By the end of the Cold War, it was more like one third of the US economy. For reference, today, the Russian economy is about 20% of the US economy at Purchasing Power Parities.

China today is not 20%, or one third, or two thirds of the US level, but as mentioned, 115%. It is already larger. And it is still growing, faster than the United States or Europe.

The world is changing. Now. This decade.

But that shift, large as it is, doesn’t mean the old problems are gone. For Europe, Russia and Islamist terrorism are the most direct potential security threats. China and dynamics in the Indo-Pacific come in addition to the other two – they do not replace them.

We do not get to choose between facing up to Russia versus China versus Islamist threats.

We also do not get to choose what relationships these threat actors may have with each other.

Those choices are theirs, not ours.

It is irrelevant whether someone in the West believes that Russia really ought to see sense and fear China and embrace the West. Maybe that would be sensible, but unless and until Russia actually behaves that way, then we cannot responsibly assume that that is the direction of travel.

In fact, the evidence of the last few years rather suggests the opposite – namely a rapprochement between Russia and China.

We may not like it, but it is not in our gift to choose the policies of other Great Powers.

We can only deal with what they do, and manage our own policies responsibly, by ensuring that we have a highly credible deterrence and defence posture, by protecting our vital interests, by remaining united and well-coordinated in our policy choices, and by applying a healthy dose of alertness and self-control in our dealings with foreign powers.

The general power shift I described is happening at the same time as we’re experiencing a major wave of new technological change.

And the biggest transformative technology is Artificial Intelligence, particularly in its contemporary form, meaning Machine Learning, which includes Deep Learning.

It is relevant to remember how world history changed in light of the steam engine, or in light of electrification, or in light of the internal combustion engine. And in more recent decades, through computing and the Internet.

All of these examples are what are called General Purpose Technologies. That is a key concept. We’re not talking about limited military technologies, or narrow civilian ones, or what I would call “narrow dual-use technologies” such as laser or thermal imaging.

General Purpose Technologies are far broader, they span a far greater range in terms of areas of application. They transform many areas of life and of economic activity – as well as the world of security and defence.

So, AI is a General Purpose Technology. And AI is going around the planet, and every state, every major organisation, private and public, knows it must invest, adapt, adopt, and move forward.

What does that mean for our security? And what is the connection with China, and indeed with other threat actors?

Well, technology diffuses. That is its wonder, and also its challenge. Humanity doesn’t get to move forward without spreading the best technologies around the world. But then no area of life is left untouched. Matters of war and peace, of the strategic balance, of military means, of coercive relations between states, and even non-state actors, that all moves along too.

Russia, for example, is working on AI for military applications.

Of course they are.

China is too.

So, what does it mean for us across the Western World?

It means the race is on. The race is on between the West and China in particular, in very visible ways. That’s what the conversation is about – transformation, new capabilities, next-generation capabilities, which will leverage AI and other new technologies.

It is important to understand the magnitude of potential future developments.

AI can improve all types of information processing, pattern recognition, prediction, for any type of data – sets of numbers, text, voice, images, video.

It has been a long time coming but now it is here. Machine Learning outperforms humans in terms of accuracy over a significant range of pattern recognition and prediction tasks.

And with appropriate “eyes and ears” on robotic systems, meaning with good sensors, and with communication technologies, we are looking at a world of intelligent connected devices, capable of determining their own courses of action to solve particular objectives.

With the ability to work effectively:

1/ In teams of machines – swarm robotics is a key expression here

2/ In mixed human-machine teams – a key expression here is human-machine teaming

3/ And alone if they become isolated from their teams and unable to communicate

All of that, in both the cyber realm and in the physical realm. With the potential of higher accuracy, and of course faster information processing and faster decision-making cycles.

This can be true for a range of civilian applications, and for military ones too. Whether it’s collaborative robotics on the factory floor – or swarms of autonomous drones in a military operation. That is the general direction of travel, with many new achievements in recent years, and with more to come.

States will necessarily invest in this space. The power implications are too great to ignore, especially once one assumes that potential adversaries will do the same. Which they will.

And with rival powers that have substantial resources and levels of ambition, we must ourselves aim at maintaining our technological edge, as much as possible, for as long as possible.

The policy question then becomes: how do states win technology races, or at least stay ahead or not fall back, within such races?

In short, we need to:

1/ get better at what we’re doing at home, and

2/ reduce the ability of foreign powers to have access to what we’re doing

This splits naturally between two dimensions: Domestic Innovation Systems, and the External Dimension.

For each dimension, I will now list 9 essential areas of work.

For domestic innovation systems:

R&D subsidies; Tertiary STEM education; Research universities; Private venture capital; Government venture capital; Government procurement; Innovation networks; Innovation clusters; Domestic industrial capacity.

For the external dimension:

IP protection (as contested); Standardization (as contested); Trade openness with non-rivals; Trade & investment restrictions on rivals; Export controls; Foreign investment screening; Counterintelligence; Espionage-related sanctions; Espionage vulnerability mitigation.

I will focus mainly on the External Dimension and develop a few examples:

1/ trade and investment restrictions on rivals

An example here is Executive Order 14032 of 3 June 2021 by the President of the United States – essentially banning US financial investments into Chinese companies involved in either the military-industrial complex of China, or that are developing surveillance technology to facilitate repression or serious human rights abuses.

You may recall that Huawei, among others, was listed. It is relevant to realise that the key companies of China’s aerospace and defence sector are there too. This is much broader than just 5G, or surveillance. We’re talking about shipbuilding, aerospace, missile technologies – and surveillance too.

The first version of that order was under President Trump, in November 2020. The one we have now, from June 2021, is slightly amended but really very similar. So, it’s important to remark that, on the US side, this is a bipartisan issue.

The rationale is simple, and in my view not controversial at all.

Why should our financial resources be invested in companies that are developing military or intelligence or surveillance technologies at the behest of foreign powers that pursue ambitions and methods that are contrary to both our interests and our values?

In the European context, we already pursue that path towards Russia. We have restrictions in place on financial investments in key Russian defence industry companies, ever since the 2014 sanctions were adopted by the European Council.

2/ foreign investment screening

Screening of Foreign Direct Investment, that is, of strategic investments in corporations in our countries, is an area of policy that has developed further in recent years.

In the United States, strengthened legislation came in 2018 – that’s the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which modernized and strengthened the key US structure in this case, which is called CFIUS, The Committee on Foreign Investment in the United States.

In the European Union, we have new EU law, namely Regulation 2019/452 of 19 March 2019 “establishing a framework for the screening of foreign direct investments into the Union”.

The regulation establishes a framework for the screening of investments from outside the Union:

1/ for Member States to each carry out (the main work happens nationally)

2/ for Member States to cooperate, with each other and with the European Commission

The regulation is a framework, it leaves a lot of leeway to Member States, but conversely this has allowed for the principles expressed in it to be very sensible and to be stated in clear language.

Article 4 of the Regulation in particular:

Member States and the Commission may consider the following areas, among others – I will just list two of them:

Critical infrastructure

Critical technologies and dual use items, including artificial intelligence, robotics, semiconductors, cybersecurity, aerospace, defence, energy storage, quantum and nuclear technologies as well as nanotechnologies and biotechnologies

If you wanted an official confirmation of what key technology areas are considered critical, this is as good a list as any. Similar lists emerge from work in the NATO context and in national strategy documents.

And Member States and the Commission may also take into account certain factors, I will just list the first one:

“whether the foreign investor is directly or indirectly controlled by the government, including state bodies or armed forces, of a third country, including through ownership structure or significant funding”

So, this is just common sense.

The recent Czech law on Foreign Investment screening seems very much to follow this common-sense spirit.

From what I’ve understood, it ensures there is mandatory notification to the government and an ability to block investments if they would result in providing effective control, by the foreign investor, over a domestic entity, and that the latter engages in manufacturing, R&D, or innovation of military equipment, or it engages in critical infrastructure, or in critical information infrastructure or essential information services, or in manufacturing or developing dual-use items.

3/ Measures against foreign state subsidies that distort competition

Another interesting development on the EU side is the proposed regulation “on foreign subsidies distorting the internal market” of 5 May 2021.

Here we’re talking about essential abilities to scrutinize and then take redressive actions in case a company on the EU market benefits from foreign state subsidies. Redressive actions could include orders to carry out divestments, for example, and the regulation would allow for the use of fines in case the company does not take appropriate remedial action.

This approach is broader-based and well within the logic of the Single Market, in which state aid by EU member states is strictly regulated. It was high time that this be applied to what is de facto state aid from foreign states.

4/ Protection of Intellectual Property: Trade Secrets

Under both US and EU law, a trade secret is information that is not generally known or discoverable by others, is maintained in secrecy by its owner (meaning a company), and it gives its owner a competitive advantage because it is secret.

Trade Secrets is one of two main approaches for companies to protect innovative ideas – the other main approach is patents, which relies on the opposite approach, namely publishing the information, but giving a legal monopoly to the patent owner to allow the patent owner to gather income from royalty fees.

Trade Secrets is an area that underwent legislative changes, in both the US and the EU, in 2016, and partly for the same reasons. In both the US and EU context, the combination of the rise of digital technologies and of the rise of China were clearly referenced reasons for strengthening legislation.

And in the case of China, we have clear evidence of cases of state-sponsored economic espionage.

In the United States, the Federal Bureau of Investigation has been very outspoken about this problem, and about its place within the broader challenge of the rise of China. To quote the Director of the FBI, Christopher Wray: “The Chinese government is fighting a generational fight to surpass our country in economic and technological leadership.”

And Wray goes on to say that the Chinese, quote, “have shown that they’re willing to steal their way up the economic ladder at our expense”.

So, we already have updated legislation for Trade Secrets, and that is a good thing. That’s just one part. There are many non-legislative measures, including programmes, training, and events to raise awareness about information security in the corporate world and in scientific research institutions for example. And this really concerns both cyber means of intrusion and human intrusions.

These four classes of policy instruments are all different, but they have a few things in common in terms of the general strategic challenge they address.

China seeks an advancement of its technological and economic power.

Distorting competition in its external trade and investments, while also aggressively acquiring technologies, whether through licit means or illicit means, and while also using state subsidies – all of these measures are tantamount to using our Western market principles against us, as a slingshot to propel China ahead of us, by making money from us, and getting our best technologies, and using the former to accelerate the latter, and the latter to enhance the former.

And so, once this is understood, the actions of China’s State-Owned Enterprises and other Chinese entities with close links to the Chinese Communist Party should be seen in a different light.

We are talking about a single-party dictatorship with major power potential and major power ambitions – in the economic and industrial realm, as well as in the military and foreign policy realm.

This does not mean that all Chinese corporations are that way, let alone all Chinese people. But it is possible to clearly identify key corporations that we should generally not be doing business with.

So, what next?

We need to start documenting in further detail who these key corporations are, their areas of activity, their linkages with key Chinese state or party institutions. Then there is the question of how they are financed and by whom, in China, in Europe, in America, and elsewhere. For instance, is it the case that European or North American capital markets are used to raise funds for these companies? Of particular interest, of course, are those companies that are engaged in supplying military, security, surveillance, or intelligence products or capabilities to the Chinese state or to the Russian state.

The more we know, the better we can target justified protective measures.

Protective measures, as mentioned, can include prohibitions on financial investments into certain key entities.

Relatedly, governments on both sides of the Atlantic may wish to block Foreign Direct Investments from those same entities, and entities associated with them.

In parallel, and this now addresses the first set of policy tools I mentioned earlier, Western nations need to provide for dynamic and competitive home-grown innovation ecosystems.

The latter require sources of capital investment they can trust – and they need more of it. It is with that intention that the US Department of Defense launched an initiative for a Trusted Capital Marketplace. Recent NATO decisions on the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Defence Innovation Fund follow a similar spirit.

Innovating more and better in crucial technologies – in Emerging and Disruptive Technologies – is now a high priority for decision makers on both sides of the Atlantic.

And the challenges related to doing so securely, bearing in mind the challenges posed by foreign powers such as Russia and China, are a major area for ongoing public policy analysis, adjustment, and maturation.

For example, are our Export Control regimes fit for purpose for the age of AI, autonomy and robotics, quantum technologies?

And do we have a proper whole-of-government approach to ensure, for example, that justified warnings from our counter-intelligence services are listened to and understood – and acted upon – across the machinery of each national government among our nations? And with coordination between our nations?

Do our corporate sectors and higher education sectors have the awareness, expertise, and inclination to detect and respond to espionage attempts, whether by cyber intrusions, or human intrusions?

And are our business and finance communities ready to work constructively on justified matters of national security and international security?

These are important considerations to have in mind as policies continue to develop and mature in the direction of better security awareness and better strategic awareness across Western democracies.

And the only way to get there is together and with a clear sense of shared responsibility for our future prosperity and for our future security.

### 2AC---AI Solves Violence

#### AI integration solves kinetic warfare

EU Institute for Security Studies 19, The European Union Institute for Security Studies (EUISS) is the Union’s agency dealing with the analysis of foreign, security and defence policy issues. Its core mission is to assist the EU and its member states in the implementation of the Common Foreign and Security Policy (CFSP), including the Common Security and Defence Policy (CSDP) as well as other external action of the Union. "The EU Nato and Artificial Intelligence" November 14. <https://www.iss.europa.eu/sites/default/files/EUISSFiles/EU%20NATO%20AI%20-%20Report.pdf> //pipk

At the event it was agreed that AI should be conceptualised as a key part of a broader nexus of emerging disruptive technologies, alongside big data, quantum computing and autonomous systems. While its exact impact remains unclear, there was consensus that AI-enabled systems would inevitably transform defence across the board. AI could enhance data management and situational awareness capacities, leading to costsavings, improved feedback control systems and decision-making, new operational concepts and greater freedom of action. On the battlefield, AI could function as an enabler across all future platforms and capabilities, with main areas of application including C2, ISR, training and logistics. As such, it would become a key factor in interoperability. AI could also change the organisational structure of military institutions in numerous – and often unpredictable – ways. In strategic terms, it could potentially lead to a reduction of the level of kinetic violence in conflict, altering the military’s role in controlling the battlefield.

### 2AC---AI Solves Decision-Making

#### AI solves military decision-making---being adopted now, effective implementation solves

Matej Tonin 19, current Slovenian Minister of Defense, was an active member of the NATO PA from 2012 to 2020. He served as rapporteur and Chairperson of the Assembly's Sub-Committee on Technology Trends and Security and as Deputy Head of the Slovenian delegation to the NATO PA. "ARTIFICIAL INTELLIGENCE: IMPLICATIONS FOR NATO’S ARMED FORCES" Report from the Sub-Committee on Technology Trends and Security. October 13. <https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf> //pipk

10. AI is already becoming a reality in armed forces around the world. All modern armed forces are, at a minimum, thinking through AI’s implications, including the ethical and legal implications, and many are introducing concrete AI solutions (see also Section IV). AI holds enormous potential for the defence sector but also presents a set of technical and non-technical challenges. Moreover, the strategic implications of AI remain unclear.

11. Tackling all opportunities, challenges, and uncertainties in depth would go beyond the scope of this report (see also Box 4). Therefore, this section delves into two key areas of opportunity (information and decision support as well as robotic autonomous systems), crucial technical and non-technical challenges, including the debate about lethal autonomous weapons systems, and some potential strategic implications.

A. INFORMATION AND DECISION SUPPORT 12. Humans generally act in an environment of incomplete information. Sometimes, plenty of information is available. In military and strategic affairs, this is decidedly not the case. Political and military leaders must act in the well-known ‘fog of war’. Information and decision support by AI systems is thus of high interest to military and strategic decision makers. Such systems can substantially increase both the pace and the quality of the processing, exploiting, and disseminating of information, as well as of human and machine decision-making.

13. In military terms, AI can considerably boost the speed of analysis and action of humans and machines. AI-enabled information and decision support systems can, for example: - vastly improve the reaction times of defensive systems against fast-acting weapon systems, such as hypersonic missiles, cyberattacks, or directed-energy weapons; - deliver actionable information faster to decision makers, which could potentially deliver a decisive edge on adversaries; - quickly discover cyber intrusions by detecting evasive malicious codes or by scanning for suspicious patterns of behaviour rather than for specific code; and - help identify attempts to manipulate citizens through disinformation campaigns.

14. AI can improve the quality of the decision making of machines, but also, and perhaps most importantly, of humans. AI’s ability to sift through today’s data-rich environment and communicate findings in a compelling manner is crucial in this respect and will become ever-more important. While human resources currently allow for the processing of, at best, 20% of the information produced today, this percentage could go down to a mere 2% (Villani, 2018). To put it in the words of an exasperated British officer, armed forces are already “swimming in sensors, drowning in data, [and] starving for insight” (White, 2019). AI solutions can help by, for example: - providing better visualisation and interpretation of data (Killion, 2018); - automatically extracting objects of interest from data feeds for follow-up actions, for example from surveillance video or satellite imagery (CRS, 2018); - establishing ‘common operating pictures’ from information which emanates from very diverse sources, arrives in very different formats, and is often redundant or incomplete (Killion, 2018); - highlighting abnormalities for follow-up investigations by comparing data points with previously developed normality models; - extracting ‘weak signals’ which do not seem alarming by themselves but may be highly significant if linked with other data (Mercier, 2018); - suggesting a menu of appropriate options and describing each option’s likely effects (Van den Bosch and Bronkhorst, 2018); and - provide insights into adversarial behaviour through foreknowledge (Demchack, 2018).

### 2AC---Yes Hybrid Threats---China

#### Chinese hybrid threats risks mischaracteriziation---being able to successfully characterize attacks is key

Hanna Smith 21, Director of Research and Analysis at the Centre of Excellence for Countering Hybrid Threats and visiting professor for the academic year 2020–2021 at the College of Europe, Bruges. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

Recent digital and technological developments have enabled many completely new tools, which have given rise to new virtual platforms that fall outside current norms and rules. These new tools have also brought unprecedented speed to all kinds of action. Interconnectivity and globalization have created new possibilities for network-based action, lowered borders, changed geopolitics and made sure that there is more data around us than ever before. New actors have emerged in international politics, who are looking to enhance their status. Authoritarian and democratic states appear to be entering into a new form of ideological battle. In this situation one can ask: what are the rules of the game? An important weapon in this new battle is hybrid threats. Hybrid threats constitute a shadow policy for authoritarian states that supports their strategic aims and is based on their strategic culture traditions. The clear dividing lines, unwritten rules, players and goals of the Cold War are history. This situation is challenging for planners, decision-makers and foresight building.

The concept of hybrid threats has entered into political normality by appearing in the discourses and documents of the EU, NATO and their member states. The concept has been examined through many different disciplinary lenses: international relations, strategic studies, security studies, military studies, history and political science – to name a few. This multidisciplinary analytical mosaic also blurs the picture of what hybrid threats really are. The Report “The Landscape of Hybrid Threats: A Conceptual Model”, issued by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) together with the European Union (EU) Commission’s Joint Research Center, uses hybrid threats as an umbrella concept, under which different types of activity occur: interference, influence, operations, campaigns and even warfare (Giannopoulos, Smith and Theocharidou, 2020). The approach adopted would enable a comprehensive analysis including civilian, political, military and academic thinking. This chapter will take the report’s conceptual model as its starting point for hybrid threat analysis.

Hybrid threats are still difficult to define, which on the one hand complicates the adoption of strategies to counter them, common positions and a holistic approach, but on the other hand gives flexibility, greater freedom to be creative and possibility to combine different disciplines and backgrounds. Consequently, the characterization of hybrid threats will help to identify real threats, potential threats and also those aspects that might look like threats but are not. Too tight definition might, in the worst case, point in the wrong direction and also tie one’s hands when it comes to responding.

There is still an ongoing debate regarding the usefulness of the concept of hybrid threats. Those saying that hybrid threats are mostly “old wine in new bottles” mean that perhaps we do not need a new concept, and we could just adjust the old ones to current circumstances. To this Frank Hoffman, who is often seen as the man behind the ‘hybrid warfare’ concept, answered in the following way: “New language and new terms aid us in thinking differently and characterizing what is truly new, hopefully without overlooking what is enduring in war. A new lexicon captures the changes better than hanging on to old terms with new meanings” (Hoffmann, 2010).

The ‘old’ in the concept of hybrid threats lies in the fact that interference and influence have always been part of international politics. Also, the technique of combining different domains like social, political, informational, military and legal ones has been part of the strategic thinking behind influence, interference and military operations. This thinking is also present in today’s activities that constitute hybrid threats. What is new, then – although anchored to traditions in the authoritarian strategic thinking – is related to today’s security environment and how it is different compared to the Cold War’s, for example. The battle between democratic and authoritarian state systems today is not as clear-cut as the division between communist and capitalist countries was during the Cold War. Furthermore, digital and technological developments have provided new platforms for influencing, new tools for both interference and influence, and have extended the domains where action happens – from the traditional military domains like land, air and sea, to cyber and space, to more comprehensive domains like culture and administration. These are all connected and, through hybrid threats activities with a targeted approach, even the best prepared states and alliances can be challenged.

The logic of interference found in hybrid threats is substantially based on authoritarian strategic culture. Strategic culture itself as a concept has been contested, but in recent years it has found its way back into security studies. It is worth noting that the Cold War juxtaposition, the bipolarity of the superpowers, crucially downplayed the relevance of national aspects relating to cooperation, competition, conflict, and war. In that way, the ‘national character’ of the enemy, which was very important before the Second World War, was downplayed during the Cold War years (Miklossy & Smith, 2020: xiii). Post-Cold War studies started to pay attention again to different domestic processes and their effects. As Glenn observed, “[t]he mid-nineties witnessed the emergence of a new school of realists that sought to move beyond the basic insights of Waltzian neorealism by investigating the interaction of systemic pressures and domestic processes in the foreign policy decision making process, thus providing a much richer explanatory account of why states choose certain foreign policies over others” (2009: 523-551). From examining national strategic cultures, the theory can also be extended to cover strategic cultures of a particular state system. Here the concept of authoritarian strategic culture comes from the studies that produce characterizations of authoritarian and totalitarian regimes (Linz, 2000; Svolik, 2012; Brooker, 2014). There are national specificities when it comes to behavior, and there are specificities that are linked to the state system. The national specificities are more difficult to define due to the fact that culture as a concept is complex. A state system is relatively easier. A state system often defines the regime type as well as its relationship to civil society, opposition and the military.

This chapter begins by presenting the characteristics of hybrid threats, as identified in the authoritarian strategic thinking specifically in relation to Russia and Chinese traditions. Those characteristics are then put into the context of decision-making following David Omand’s Situation awareness, Explanation, Estimate and Strategic notice (SEES) model. In the third part, the challenges that the new information environment presents us are considered, and finally the chapter draws some conclusions relating to allied decision-making.

Hybrid Threats and Strategic Thinking As mentioned in the introduction, this chapter takes as its starting point the report “The landscape of Hybrid Threats: A conceptual model”. The report does not claim to be an exhaustive source for the description of all the characteristics that hybrid threats might have, and there might be many more that have to do with the changing nature of the phenomenon. However, the report does identify five characteristics deemed to be the most important with respect to the challenges they pose to decision-making: • Usage of multiple synchronized tools, used to create linear and non-linear effects; • Ability to create ambiguity with plausible or implausible deniability and to hide true intent; • Deliberate threshold manipulation and the use of grey zones like borders between war and peace, friend and enemy, virtual and real, internal and external, etc; • Exploitation of the seams of democratic societies and the different jurisdictions (local, state, international); • Use of decoys. These five challenges are all related to Russian and Chinese interference and influence traditions, which will be presented in the following sections. In turn, they are part of wider strategic culture, which is the product of a centuries-long dialogue between a people and its history (Gray, 2006: 15). Strategic culture is closely interlinked with the idea of national interests in a spatial context that is defined by potential threats, perceptions of friends and foes, traditions of alliances, and institutional linkages (Miklossy & Smith, 2020: 263).

Traditions of Chinese strategic thinking Since uncovering strategic culture is beyond the scope of this chapter, the approach is to present some dominant ideas that are still present today in Chinese thinking relating to interference, influence and winning conflicts and wars. The Chinese thinking presented here is based on three books; On Strategy Studies (2006) published by the People’s Liberation Army (PLA), Political Work Guidelines of the People’s Liberation Army (2003), where the “Three Warfares” concept is introduced, and The seven military classics of Ancient China (2017), which presents seven texts from different times seen as cornerstones of Chinese military tradition. This is particularly relevant since President Xi Jingping has forbidden the use of foreign theory books in education and has mandated turning back to their own classics including those on strategy (Nojonen, 2019). Therefore, Chinese practitioners of strategy are actively studying their own classics in building a professional identity and practices based on the particular traditional conceptualization of the Chinese strategy work (Nojonen, 2019).

The book On Strategy Studies, published in Chinese, introduces the concept of “supraplanning”: a dynamic process towards a goal – and not a rigid adherence to a sequence of steps that is forever fixed and precisely worked out in advance. The authors outline three factors that determine the strategic behavior of the Chinese military: strategic thinking, strategic environment and military capacity. The book makes a point that the aim is “to lure the other side into developing misperceptions…and to [establish for oneself] a strategically advantageous position by producing various kinds of false phenomena in an organized and planned manner with the smallest cost in manpower and materials” (Detweiler, 2009: 10).

In analyzing Chinese strategic behavior, the authors argue that the tradition, understanding and practice of stratagems is the dominant pattern of Chinese strategy thinking. Based on the book, the characteristics of Chinese supraplanning are: a) resourcefulness and decisiveness; b) deep stratagems and distant deliberations; c) comprehensive planning and preparations; d) flexibility and ingenuity. It is important to note that different concepts found in traditional Chinese strategic thinking are presented in a dialectic way, such as “weakness and strength”, and “clandestine manoeuvres and open operations”. This means that concepts are not strictly defined, but rather remain borderless and ambivalent, creating ambiguity. Also, these concepts can be nouns and verbs at the same time; in other words, they can be both abstractions of cognitive processes as well as actual practices. This means that a solid picture of each given situation might be very difficult to form without a profound knowledge of Chinese language (Nojonen, 2019).

Also, the more well know Chinese concept of “Three Warfares”, in the book Political Work Guidelines, comprises three different components: Psychological Warfare, Public Opinion Warfare and Legal Warfare. The Three Warfare concept was first made official in the revisions of the PLA’s Political Work Regulations in 2003. - Psychological Warfare is defined as operations that achieve political and military aims by influencing a target’s psychology and behavior through the distribution of specific information. Situational awareness can be blurred with informational manipulation, and different biases can be supported. In this respect, the ‘targets’ are practitioners and decision-makers. Psychological Warfare methods include deterrence, coercion, deception, instigation, seduction, bribery, inducement and confusion. These methods are part of both theoretical and doctrinal descriptions. - Public Opinion Warfare is defined as operations aimed at influencing both domestic and international support with the use of selective information delivered through different media. This is different from psychological warfare in the way that it aims to control the masses. The main channels for this type of activity are the internet and traditional media sources, such as broadcasting and newspapers. Towards the public opinion, warfare concept channels also include international organizations and academic forums that can be used from within under a tailor-made approach. - Legal Warfare is used to attain legal superiority by using domestic and international law to gain a political initiative or military advantage. Rather than viewing law as a method of rational order- making, legal warfare looks for ways to use legal advantage to influence targets by delivering the effects of interference, response, defeat, deterrence, or defense via legal means, including through national or international channels.

The third book, The seven military classics of Ancient China, gives a comprehensive picture from a historical perspective of how Chinese rulers and generals have analyzed the best ways to keep power, get power, conquer land, defeat the enemy and gain control. The book includes Sun Tzu’s famous “Art of War”, and Huang Shigong’s “Three Strategies”, which discusses the Art of War. In the latter text, for example, the line “Follow their (enemy) trends in order to break them. Be wild with your words in order for them to make mistakes. Surround them with your net in order to catch them”, could be applied to today’s security environment, where the manipulation of information is based on the assumption that decision-makers will make mistakes that favor the actors providing misinformation. All these texts have psychological elements, search for weaknesses and look for ways to covertly succeed.

This snapshot of Chinese strategic thinking already shows that it will be very hard from outside China to identify actions that are seen and planned by Beijing to be borderless and ambivalent. Furthermore, different levels of decision-making are the main target. The various tools are designed to work in the way that situational awareness is blurred and context is lost, which means that estimates, warnings and preparedness in the target are incomplete.

### 2AC---Yes Hybrid Threats---Russia

#### Russia is weaponizing AI through hybrid warfare---that undermines NATO decision-making

Franz-Stefan Gady 21, Research Fellow for Cyber, Space and Future Conflict, International Institute for Strategic Studies. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

This chapter seeks to offer preliminary answers to two questions. First, to what degree will Artificial Intelligence (AI)-enabled information warfare exacerbate hybrid threats to NATO decision-making? Second, what can NATO countries do to alleviate the threat? To narrow the research scope, this chapter will principally look at threats posed by Russian AI-enabled information warfare operations under the concept of gibridnaya voyna. The study argues that given that AI-enabled information warfare has the potential to amplify societal polarization, elite disagreement within domestic politics, and reshape the perception of the “Russian threat” in NATO member countries, it can have a direct negative impact on national and NATO decision-making. Such operations, however, only amplify existing symptoms of polarization and disagreement found within NATO member states and are not their root causes. The chapter concludes that NATO must better integrate tech-centric so-called “whack-a-troll” tactics with a whole-of-nation strategy to better safe-guard NATO decision-making and alliance cohesion. Renewed discussion of whole-of-society defense concepts to inform national security strategies may be useful in this regard.

Introduction NATO defines hybrid threats as threats that “combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces” (2019). Such hybrid methods are used to blur the line between war and peace and “attempt to sow doubts in the minds of target populations.” NATO further emphasizes that “[t]he speed, scale and intensity of hybrid threats have increased in recent years.” The latter can partially be traced back to various technological advances including in the fields of Artificial Intelligence (AI) and offensive cyber capabilities, utilized in conjunction with deliberate attempts by competitor nations to undermine the political cohesion of NATO member states from within.

Hybrid threats pose a number of unique challenges to political decision-making within both NATO member states and the Alliance’s various deliberative bodies, where decisions are based on the principle of consensus preceded by consultation processes (NATO, 2020). In particular, meddling by outside powers in political processes by means of influence operations, broadly defined as “organized attempts to achieve a specific effect among a target audience,” is one of the top concerns of NATO leadership (Thomas et al., 2020). In particular, Russian tactical-operational influence operations under the concept of gibridnaya voyna (‘hybrid warfare’) have been receiving a great deal of attention since 2014. As Ofer Fridman notes, such operations target society at large, seeking to undermine political cohesion in an adversary state by employing methods that amplify the divisions and polarizations among its citizens (2018).

Definitional confusion has plagued the discussion on hybrid warfare. Fridman, who sketches the conceptual evolution of the term in both the West and Russia, points out that at least three different phenomena have been described as hybrid warfare in past years with no agreed upon definition. Indeed, the term ‘hybrid warfare’ itself may at this point obfuscate rather than clarify modern conflict characteristics. As Fridman argues: “Despite the political usefulness of the term hybrid warfare, it would appear that Russian and Western military professionals now recognize that the term is next to useless for describing the real nature of contemporary conflicts, leading them to promote more specific definitions, such as information warfare, cyber warfare, which are now prevalent in the West, or new-generationwarfare, which is currently prevalent in Russia” (2018: 157).

Indeed, the Russian Chief of the General Staff, General Valery Gerasimov, has publicly aimed to draw a distinction between new-generation warfare and hybrid warfare with the former – given its emphasis on military capabilities – being the main focus of the Russian Armed Forces (Fridman, 2018).

Nonetheless, it is evident from a review of Russian military literature that hybrid warfare focused on weakening societal cohesion of an opponent still retains a prominent spot in Russian national security thinking. For example, a 2015 article on future warfare published in the widely-read journal of the Russian Ministry of Defence stated in strong terms the centrality of information to the Russian understanding of future war, asserting that “it is precisely the information-psychological struggle which will, in the main, create the preconditions for the achievement of victory [in future warfare]”. The article, authored by two frequent contributors on future warfare, continued: “…the achievement of strategic objectives in future wars will be impossible without the establishment of information dominance over the enemy. In future wars, special disinformation operations and [operations for] misleading the military-political leadership of the other side will include a system of interconnected and carefully-agreed upon large-scale measures according to the plan of new-type war (‘hybrid war’), including the use of various means of actions upon the personnel of the armed forces and population of the state with the objective of creating internal tension (schism) in society. Information-psychological operations in future war will pursue by non-forceful means the objective of achieving the significant weakening of the military potential of the enemy by means of affecting his information processes, misleading [him], demoralizing the population and the personnel of the armed forces” (Bogdanov and Chekinov, 2015: 45)

As part of such future Russian gibridnaya voyna campaigns, the effective integration of AI with cyber capabilities that enable faster and more precise weaponization of information has the potential to compromise and undermine NATO decision-making at multiple levels. This chapter consequently seeks to offer preliminary answers to two questions in this regard. First, to what degree will AI-enabled information warfare1 exacerbate hybrid threats to NATO decision-making? Second, what can NATO countries do to alleviate the threat?

To narrow the research scope, this chapter will principally look at threats posed by Russian influence operations under the concept of gibridnaya voyna.

Factors Influencing NATO Decision-Making In order to answer to the above questions, it is first necessary to outline the various influences that impact allied decision-making within NATO. According a recent RAND study, member states’ decision-making processes on their own participation in NATO operations can be broadly divided into three categories: • Domestic politics; • Perception of the Russian threat; • Alliance dynamics (Binnendijk and Priebe, 2019).

Notably, RAND finds that domestic politics and perceptions of the Russian threat have the larger impact in decision-making processes involving an unconventional (i.e. hybrid) attack on a NATO country. In the future, such an attack would undoubtedly feature AI-enabled information warfare as part of gibridnaya voyna embedded within a new-generation warfare campaign. Consequently, this chapter will primarily focus on domestic politics and perceptions of the Russian threat to illustrate Russian tactical-operational AI-enabled information warfare.

According to the RAND study, domestic political considerations that influence decision-making regarding support or opposition to NATO military action in an unconventional environment are impacted by a number of factors, including the proximity of public elections, general public support for a particular course of action, elite agreement or disagreement (coalition governments can be particularly vulnerable in this case), and a centralized or decentralized foreign policy decision-making structure. Perceptions of the Russian threat in turn are also subject to a number of factors including perceptions of Moscow’s aims and motivations, escalation risks, vulnerabilities to Russian economic sanctions as well as military retaliations, and competing national security demands (Binnendijk and Priebe, 2019).

Most relevant for this chapter is that in both instances – domestic politics and perceptions of the Russian threat – AI-enabled information operations have the potential to influence factors in favor of Russia. For example, such operations could expand the audience reach of NATO-skeptical parties during election seasons, or in advance of a parliamentary vote in order to undermine elite consensus on anti-Russian actions. Alternatively, with the help of a carefully crafted ‘what aboutism’ narrative employed part of a wider disinformation operation, Moscow could amplify disagreement over aggressive Russian actions within a target country by emphasizing online that Russia, like any other country, is merely pursuing legitimate selfinterest.

AI-Enabled Information Warfare AI-enabled information warfare entails the use of algorithms capable of processing and learning from big data to execute attacks against specific targets autonomously or semi-autonomously in order to achieve a desired effect in the information space. 2 The terms ‘autonomously’ and ‘semi-autonomously’ describe respectively the ability of the algorithm without or with (limited) human intervention to learn from vast amounts of data in order to execute polymorphic attacks on multiple fronts in the information space (for example, simultaneous attacks on a microblogging site synchronized with emails phishing attacks), in which the algorithm is capable of changing its identifiable features (for example, by creating multiple malicious online identities fitted with unique malware packages). The most relevant media for AI-enabled information warfare are audio, text and video (Giles and Hartmann, 2020). Furthermore, AI-enabled information operations target all interrelated dimensions of the information environment – physical, informational, and cognitive/emotional. Herbert Lin and Jaclyn Kerr define the information environment as, the “aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information” (2019: 4).

AI-enabled information warfare methods may plausibly be deployed in various other ways. For example, AIenabled algorithms permit the building of realistic simulations of individuals “to test every individual’s reaction to events (both virtual and real), advertising, political campaigns, and psychological operations, and even to guess what might go viral through person-to-person interactions” (Libicki, 2017: 52). Such simulations could be created by deploying an algorithm capable of pattern recognition to study the social media behavior of a select target group of individuals in a specific country. This in turn could be used to create personalized phishing emails for social engineering attacks, but also to create so-called ‘deepfakes’ to gain access to sensitive systems or to facilitate the spreading of disinformation. Another example is the use of bots in order to ’hijack’ public perceptions: “Bots, trolls, and sock puppets can invent new ‘facts’ out of thin air leading to a polarized society and a culture of mistrust” (Wright, 2019: 318). The main objective behind creating alternate facts would not be to create a convincing alternative narrative – which is an objective of strategic communications – but rather to erode the solidarity of groups facing the same threat by playing on the fears and anxieties of individuals (Libicki, 2017).

In sum, AI-enabled information warfare differs from ‘regular’ information warfare in four crucial areas: 1. Speed: AI can accelerate the pace of operations by, for example, faster identifying targets due to the expedited operationalization of cyber intelligence, surveillance and reconnaissance (ISR) data as a result of increased pattern recognition capabilities of algorithms. 2. Scope: AI can expand the scope of information warfare operations by semi-autonomously or autonomously executing polymorphic attacks on multiple platforms with the help of bots, trolls, or sock puppets. 3. Scale: AI can increase the chances of a particular message or narrative going ‘viral’ in the information space by, for example, self-learning algorithms ‘wargaming’ the potential impact of specific content online, or AI-enabled facial recognition software that is capable of recognizing emotional states of individual humans. 4. Sophistication: AI can not only increase the sophistication of microtargeting processes, but also facilitate the creation of ever more convincing synthetic media products (such as ‘deepfakes’) with the support of Generative Adversarial Networks (GANs) where it is increasingly difficult to separate real from synthetic identities (Rocca, 2019).

Since AI is both scalable and effective, it is likely to be of significant utility to those seeking to undermine Western democracies because it will permit adversaries to avoid making tradeoffs between scale and effectiveness. In particular, AI will likely allow adversaries to expand exponentially the scale and rate of attacks, while also increasing the number of targets (Rocca, 2019). In addition, the following factors are all likely to enhance the utility of AI in information warfare: societies’ growing dependence on cyberspace as a news source; citizens’ increased reliance on social media; the difficulties individuals face in distinguishing between fake and genuine news sources; the unprecedented levels of access to information; and the speed at which information can be spread between individuals (Giles and Hartmann, 2020).

AI, however, is no panacea for influence operations. The impact of AI-enabled information warfare will largely depend on the quality of input data on the one hand, and continue to be contingent on analogue factors that may be too difficult for algorithms to effectively process on the other (for instance, various cultural and historical factors that may impact a society’s reaction to a particular event).

Furthermore, an overreliance on AI-enabled technology, in particular for conducting information warfare operations in cyberspace, may be misguided given the uncertainty surrounding the degree to which AI will favor the offense or defense (Dafoe and Garfinkel, 2019b). Building on the literature analyzing ‘regular’ or conventional cyber attack and defense operations (given that AI-enabled information warfare operations will mainly be conducted through this domain), broad generalizations on the subject are misplaced. As one analysis regarding the offense-defense balance in cyberspace puts it: “Sweeping claims about the offensedefense balance in cyberspace are misguided because the balance can be assessed only with respect to specific organizational skills and technologies” (Slayton, 2016: 72).

Nevertheless, there is some evidence that certain methods appear to favor the offensive. As a digital forensics expert notes regarding deepfake technology, “the adversary will always win, you will always be able to create a compelling fake image, or video, but the ability to do that if we are successful on the forensics side is going to take more time, more effort, more skill and more risk” (Giles and Hartmann, 2020: 236). Another analysis notes that scaling effects will likely be an important factor in determining the offensedefense balance (Dafoe and Garfinkel, 2019a). Nonetheless, it is unclear whether, for example, increased automation alone will ultimately favor the attacker or defender. Given that AI-enabled information warfare will be carried out principally through cyberspace, the uncertainty surrounding presumed technical solutions should therefore be kept in mind by policymakers.

If no discernible offensive advantage can be achieved, there is the risk of an information war of attrition with no clear winner but with excessive collateral damage sustained by society overall. The series of Chinesebacked Covid-19 disinformation campaigns executed in 2020 are a good example of this, having inflicted lasting damage on the information spaces of a number of Western democracies despite the adoption of successful countermeasures by governments (Ha & Cho, 2020). As these campaigns have shown, an information warfare stalemate would likely be more harmful to democratic societies that assume the presence of free speech as a norm than to authoritarian societies where the flow of information is under tighter control, and where consequently a disruption of the information space will have fewer consequences.

### 2AC---War Outweighs

#### War makes everything else harder to manage

Bryan Walsh 2/26, Editor, Future Perfect, Vox. "The war in Ukraine could portend the end of the “long peace”"The war in Ukraine could portend the end of the “long peace” <https://www.vox.com/2022/2/26/22951016/russia-ukraine-long-peace-nuclear-weapons-global-development> //pipk

Those abandoned fallout shelters were on my mind on Wednesday night as I watched Russia overturn decades of seemingly settled international policy with an invasion of Ukraine that was as premeditated as it was shocking. What sets this action apart from the countless conflicts, large and small, that have unfolded over recent decades, is the specter of nuclear weapons.

That was implicit in Russia’s decision to exercise its strategic nuclear forces in the leadup to the invasion, in Putin’s absurd casus belli claim that Ukraine was going to develop its own nuclear weapons, in his threat that countries that interfered with Russian actions would face “consequences you have never seen.” As Roger Cohen pointed out in the New York Times, Putin’s speech “seemed to come closer to threatening nuclear war than any statement from a major world leader in recent decades.”

The irony is that one of the reasons Ukraine was vulnerable to a Russian invasion is that it does not possess nuclear weapons. It agreed in 1994 to give up Soviet nukes that had been left in its territory after the USSR’s breakup in exchange for an agreement that the US, the UK, and Russia would guarantee its security. And one of the reasons that Putin could invade knowing that international opposition would be largely limited to diplomatic and financial tools was that Russia still possesses the world’s largest nuclear arsenal.

It has also retained strategic ambiguity about just when and why it would use those weapons, including the possibility it would threaten a nuclear strike if it were on the losing side of a conventional conflict with NATO.

As Vox’s Zack Beauchamp writes, what we’re seeing is an illustration of the “stability-instability paradox” of nuclear weapons. As the chance of nuclear conflict declines, the theory holds, the risk of conventional war increases, and as the likelihood of nuclear conflict increases, the risk of conventional war declines. That in turn helps explain another paradox: why the decades following the introduction of nuclear weapons — weapons that, in their most maximalist effect, could conceivably bring an end to human civilization — also saw a historic fall in the number of war-related deaths around the world.

Chart of battle deaths 1945-2016

Our World in Data

These decades go by another name: “the long peace.” The name can be a bit misleading — for much of the world, these years have been anything but peaceful, with the number of discrete conflicts beginning to rise in the 1960s and staying high ever since.

These ranged from large conflicts like America’s decade in Vietnam and the 1980s Iran-Iraq war to countless small skirmishes, often conflicts within countries, that barely penetrated the international media. But compared to the blood-stained decades that marked the first half of the 20th century — which saw more than 100 million deaths in World Wars I and II combined — let alone humanity’s tremendously violent past, these years have indeed been a holiday from history.

And if the invasion of Ukraine marks a decisive end to that holiday, as some experts have suggested, we risk losing far more than peace.

The wages of peace

When Future Perfect was launched in 2018, Vox’s Dylan Matthews laid out a founding question: “What topics would we write about if our only instruction was to write about the most important stuff in the world?”

The years that followed provided some of the answers: the battle against global poverty and the common diseases that still kill too many of the world’s poorest; the growth of effective altruism and the rigorous movement to do the most good per dollar; the expansion of moral concern from tribe and nation to all of humanity and even non-human species; and yes, occasionally, the existential threat of superintelligent AI.

What these topics have in common is that they all flourish best in peace.

The last half-century or more hasn’t just seen a historic reduction in the casualties of war. It’s also witnessed an unprecedented expansion in human prosperity, as measured in health, wealth, and education. It’s an expansion that is far from perfect and far from complete, but one that has opened the door, even just a crack, to a future that truly could be perfect.

That progress, I would argue, depends on peace. Unchecked war is the great destroyer of human value. One estimate from 2019 put the economic impact of violence and conflict at $14.4 trillion that year, equivalent to more than 10 percent of gross global GDP.

But dollar figures are only one way of counting the destruction. A world where borders can once again be remade with force, where countries and their citizens no longer feel secure from better-armed neighbors, is one where the broader goals Future Perfect covers (and values) will be harder to achieve, where the circle of moral concern could shrink rather than grow. It is a return to barbarity.

### 2AC---Deterrence Solves Climate

#### Deterrence solves climate change

Shruti Samala 21, Staff Assistant Intern for the Wilson Center's Environmental Change and Security Program. "Climate Change and Nuclear War: Existential Threats on a “Split Screen”" October 26. <https://www.newsecuritybeat.org/2021/10/climate-change-nuclear-war-existential-threats-split-screen/> //pipk

“In international relations today, we face two truly existential threats—in climate change and in nuclear war,” says Robert Litwak, Senior Vice President for Scholars and Director of International Security Studies, in a new episode of Wilson NOW. The interview with Litwak focuses on his new article, “Geostrategic Competition and Climate Change: Avoiding the Unmanageable,” recently published in 21st Century Diplomacy: Foreign Policy is Climate Policy.

Climate catastrophe and nuclear war are often conceptualized as separate and distinct—as if on a split screen, says Litwak. At this critical juncture—when “the risk of conflict between the United States and its Great Power rivals, China and Russia, is at the highest point since the end of the Cold War”—the two crises must be understood as interconnected.

Curtailing unrestrained geostrategic competition is a precondition for averting the climate crisis, says Litwak. “…if we don’t get a handle on the geostrategic competition, which has its own dire potential consequences if conflict were to break out, we will be nowhere on climate. We will not be able to have the collective action necessary, and we have a narrow window for action on the climate piece. The geostrategic piece has created such virulent relations that it precludes the kind of global cooperation among U.S., Russia, and China that we need to address the climate threat.”

In theory, great powers can compartmentalize climate change from long standing geopolitical pressures in order to jointly curb global carbon emissions, says Litwak. But China and the United States espouse opposing perspectives on climate diplomacy. China views climate change mitigation through a transactional diplomacy lens—that is, international collaboration to decarbonize the economy is not dissevered from traditional geostrategic dynamics but rather a means to simultaneously pursue parochial state goals. In contrast, the U.S. position is that climate change transcends national interests, and should not be brandished as a “geopolitical weapon” or ideological tool, says Litwak.

These conflicting standpoints play out against the backdrop of heightened tensions between the United States and its nuclear-armed adversaries, China and Russia. A “new calculus of risk” has emerged in geopolitics, says Litwak. First, strategic competition is territorial, not ideological, in nature: Superpowers are jockeying for power over border areas of core national interest, namely Taiwan and the South China Sea for China and Ukraine for Russia. Second, the development of advanced technologies and the extension of competition into new domains (cyber and outer space) create new escalatory risks. “The nuclear states are committed to nuclear modernization with new types of weapons that may affect strategic stability, and create an incentive for one side or the other to go first in a crisis. And up until now, the sine qua non of strategic stability has been essentially mutual vulnerability,” says Litwak. “That calculus may be changing with new capabilities.”

The tensions between the United States and Russia and China are not likely to be eliminated, says Litwak, but must be managed for there to be any possibility of opening lines of dialogue around climate between the two warring factions. Litwak shares key pathways to maintain deterrence: 1) settle territorial disputes that serve as major flashpoints for conflict; 2) revive the arms control architecture of the 1980s and 90s, which stipulated frameworks for nuclear modernization; and 3) engage in international summitry in order to establish “rules of the road, guard rails, basic principles to govern relations” that manage unrestrained geostrategic competition.

At the 1985 Geneva summit, says Litwak, President Ronald Reagan asked Soviet Union leader Mikhail Gorbachev if the two nations could put aside their differences and unite together in the event of an alien invasion. Climate change is analogous to this extraterrestrial attack, says Litwak. The fundamental question now is whether unconstrained geostrategic competition will hinder concerted action—or will the superpowers work together to forestall the worst effects of climate ruin?

## Cooperation Advantage

### 2AC---NATO AI Coop Solves Democracy

#### NATO AI cooperation is key to preserve democracy

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

The ongoing technological transformation has not only renewed great powers’ longforgotten competition in areas like technology, with the so-called AI race,330 but it has also given rise to new instruments for political competition and influence.331 The effect of these instruments is particularly subtle, because they undermine the very principles and institutions – such as democracy, freedom of speech and free markets – on which NATO is built and which, as an Alliance, it tries to promote.

Propaganda, disinformation, deception and counter-intelligence have always existed. However, the possibility of applying emerging technologies with disruptive potential to these domains is relatively unprecedented.332 For instance, forensic evidence related to popular digital platforms like WeChat and TikTok shows that specific hashtags, accounts or information have been suppressed by foreign actors or governments, likely for political reasons.333 Similarly, in the past few years, autocratic regimes have recurrently relied on chatbots, troll farms and diffusion of disinformation through Facebook or Twitter with a view to altering political competition within, and outside, NATO.

Second, key technologies related to AI, ML and BD, such as facial and speech recognition software, provide new opportunities for autocratic rulers to curtail individual freedoms, impose human rights abuses and implement societal control measures which would be deemed unacceptable within NATO. However, some countries are exporting those technologies around the world, thus making undermining democracy and freedom not only at home but also abroad.334

Last but not least, while economic competition and economic intelligence have long characterized statecraft and international relations, in an age when technology yields accelerating returns, adversaries and competitors can (and do) exploit free markets and open societies so as to steer chaos and appropriate foreign technology. This has nefarious implications for competitiveness as well as national security, given the dual nature of many technologies at hand.335

These are issues on which NATO and its Allies are in a sense caught unprepared. The dominant consensus has long held that digital technologies would undermine autocratic rule, and that that state-sponsored economic activities would struggle to keep pace with free markets.336 Recent history has proved both assumptions wrong. Firewalls can permit autocratic countries to control their internal flow of information. ML and BD can increase, rather than undermine, societal control. Free markets and open societies are vulnerable to uncompetitive and unfair measures and, such as theft of intellectual property or illicit transfer of technology, as well as to disinformation and propaganda, which are made more effective by digital platforms.

Whether these are examples of hybrid threats is an important discussion, which cannot be addressed here.337 NATO Allies, however, have important issues to discuss. Anti-fake software. We are all potential victims of disinformation. The evolution of disinformation, thanks to the development of generative adversian networks and the emergence of so-called deepfakes – videos that create artificial speeches over video clips of notable public individuals – is particularly worrying. For NATO, deepfakes could represent an existential threat as trust in political and social institutions could be dramatically undermined. One layer of defence for NATO could consist in promoting the development and adoption of an anti-fake software – i.e., one that can be easily installed on anyone’s phone or desktop as an alert system against seemingly illegitimate content. This could be funded as a pilot project or through a Grand Challenge. The goal would be to enable all individuals to be protected from disinformation attacks. Self-evidently, the software, its code as well as its parameters must be sufficiently open and transparent to enable public scrutiny.338

Algorithmic principles. NATO Allies have a strong interest in agreeing on, and setting out, a series of principles and actions to stop their companies supporting, even unintentionally, the rise of digital authoritarianism. In particular, it is important to ensure that their technologies or services be prevented from enabling the use of AI for purposes which go against NATO values and principles, such as mass societal control or suppression of free speech.

Cyber security and investments screening. Cyber attacks, theft of intellectual property as well as well illicit transfer of technology, including through mergers and acquisitions of foreign companies, have grown exponentially in recent years. Such tactics undermine economic competition and are extremely perilous from a security perspective, given that they make it possible to bypass measures such as technology export control regimes. NATO and its Allies have a strong interest in strengthening the cyber defence of their companies. This may imply, for start-ups and small and medium enterprises, various incentives to build up their cyber security, as well as direct government support. At the same time, a NATOwide effort towards the screening of foreign companies’ investments and acquisitions is important to counter illicit transfer of technology: cooperation with the European Union would be important in this respect.339

A technological alliance of democracies. As highlighted in previous sections, the challenge facing NATO and its Allies is massive, sudden, subtle and multidimensional. In some areas, intra-Alliance cooperation and coordination combined with powerful initiatives will not suffice, as close work with the private sector and with external partners will be necessary. This is why a group of prominent researchers have proposed a technological alliance of democracies, to better address the threats and challenges we are facing.340 The role of NATO outside its borders – and the Euro-Atlantic area more generally – is admittedly a sensitive issue, on which multiple perspectives and sensitivities co-exist. However, there is room for the Alliance to play a more proactive role around the world in upholding, mostly through diplomacy, the very principles on which it is based: democracy, free markets, rule of law and human rights.

### 2AC---US AI Coop key to Democracy

#### US cooperation with allies on AI key to democracy

Andrew Imbrie et al 20, Andrew Imbrie Ryan Fedasiuk Catherine Aiken Tarun Chhabra Husanjot Chahal. Center for Security and Emerging Technology (CSET) at Georgetown’s Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. February. "Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI" //pipk

The United States has long benefited from its network of allies and partners that contribute forces, specialized capabilities, and legitimacy to U.S. leadership in the world. In recent years, however, this network has come under strain. Disputes over burden sharing and mutual recriminations have raised questions about the cohesion and durability of existing alliance structures. Recent U.S. policy shifts and withdrawal from certain international agreements have deepened fears that the United States no longer sees its allies and partners as central to U.S. strategic objectives and national security.

America’s alliances are weakening at a time of growing competition between democratic nations and authoritarian regimes. Authoritarian regimes are surviving longer and becoming more adept at using AI-enabled surveillance and censorship technologies to export their values abroad.5 China and Russia present a significant challenge to liberal democratic societies.6 A world in which China and Russia deploy AI to widen the net of information controls is a world of diminished rights and protections for the individual, fewer safeguards for privacy and the rule of law, more data exploitation, and limited opportunities for judicial redress or public dissent.7

Despite the importance of alliances in promoting democratic values and protecting against a mounting authoritarian challenge, the United States lacks a strategic approach for cooperating with allies and other like-minded partners on AI.

#### US EU cooperation on AI key to global US leadership and democratic AI

Julia Voo and Lauren Zabierek 20, Cyber Fellow, leads the team behind Belfer’s National Cyber Power Index, and is the former Research Director for the Belfer Center’s new China Cyber Policy Initiative. Her areas of research include the Digital Silk Road, industrial policy, and technical standards for strategic technologies. Voo also has research affiliations with the Future of Humanity Institute (Oxford), the Hague Program for Cyber Norms (Leiden), and the China-Africa Research Initiative (Johns Hopkins). A 2019 graduate of Harvard Kennedy School’s mid-career Master in Public Administration program, Julia served earlier at the British Embassy in Beijing where she covered China’s cyber and artificial intelligence policy from a commercial perspective, technical standards, and other trade policy issues. Executive Director of the Cyber Project at Harvard Kennedy School’s Belfer Center where she leads research and programming on domestic and international cyber and emerging technology policy issues; her driving vision for the Project is “Cybersecurity is National Security.” She comes to this role as a 2019 graduate of the Kennedy School’s mid-career MPA program. Lauren served as an intelligence officer in the United States Air Force at the beginning of her career. Later, as a civilian intelligence analyst with the National Geospatial Intelligence Agency (NGA) assigned to the Office of Counterterrorism, she completed three war zone deployments where she worked to identify and dismantle terror networks. The Cyber Project Belfer Center for Science and International Affairs Harvard Kennedy School. "The Case for Increased Transatlantic Cooperation on Artificial Intelligence" August. <https://www.belfercenter.org/sites/default/files/2020-08/TransatlanticAI.pdf> //pipk

The next decade will be a decisive time for the US to shape its future role in the world. Democracies are being tested and toyed with by malign powers, as seen in the form of Russian interference in the 2016 US Presidential elections and subsequent disinformation campaigns by other nations. Great power politics and the national security implications of emerging technologies, such as AI, are breaking up supply chains and further fragmenting the internet. We’re witnessing shocks to the liberal economic order and global governance as a result of several economic crises and the aftermath of the biggest public health crisis in a century. Societies across the world will be looking to develop and implement new technology to deal with crises and recover from economic losses faster. The rise of revisionist powers and the transformative potential of emerging technologies means that the US and its European allies need to prioritize investing in capabilities and its relationships to ensure that emerging technologies align with liberal, democratic values. While the US currently maintains a slight edge in research and development of AI capabilities, that advantage is eroding as a result of a shortage of AI talent, lack of engagement between the federal government, academia, and the private sector, and overall gaps in federal government funding. US innovation has its roots in an open and multicultural society. American leadership in innovation is the result of decades of attracting, training, and recruiting the brightest minds in the world. While recognizing that there are some national security risks, efforts to cut off the flow of students will be detrimental to long-term US innovative capabilities. The European Union while maintaining its role as a leader in AI ethical guidelines, also faces challenges stemming from a lack of talent as well as insufficient funding and uncoordinated AI expertise and application across the Member States. Moreover, the EU suffers from other institutional challenges that are most glaringly demonstrated by the UK’s vote to leave the EU in 2016—which unbeknownst at the time dealt a major blow to the EU’s AI ecosystem. The US and EU need to enhance cooperation in the development and application of AI in healthcare, environmental science, and defense. When the US and EU work together on global challenges such as healthcare and environment science, the rest of the world benefits. And there are other key geopolitical challenges that the US and EU face that can only be balanced together. We are delighted to share with you this analysis of the AI landscape between the US and EU, written and researched by our students working with the Cyber Project and China Cyber Policy Initiative, Christie Lawrence and Sean Cordey. We feel this report provides a strong evidence base for further collaboration, and puts forth thoughtful recommendations. The importance of the transatlantic relationship cannot be understated. The world needs strong leadership in these uncertain times and the US and EU bring unique strengths to the table that collaboratively can strengthen the other’s advantage in the face of unprecedented technological and geopolitical challenges. The US and the EU need to work together.

#### Plan builds a coalition that spills over to broader international collaboration---solves democratic alternatives to Chinese AI---countries will follow the model

Andrew Imbrie et al 20, Andrew Imbrie Ryan Fedasiuk Catherine Aiken Tarun Chhabra Husanjot Chahal. Center for Security and Emerging Technology (CSET) at Georgetown’s Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. February. "Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI" //pipk

The United States has a vested interest in setting the rules of the road for artificial intelligence. Western countries have already taken the lead in developing principles governing the application of artificial intelligence. China has produced its own set of principles and engages actively in international bodies, such as the International Telecommunication Union (ITU) and the 3rd Generation Partnership Project (3GPP), to establish standards for mobile network technologies and the future governance of AI.

By assuming leadership in AI, the United States and its allies face risks and opportunities. The risks are twofold. On the one hand, standard setting could become a casualty of geopolitical competition as leading countries precipitate a race to the bottom. On the other hand, China already asserts its principles and standards through a variety of multilateral fora. The opportunity is that the United States and its allies can act now to set global standards for AI reflecting and supporting human rights and liberal democratic values, while addressing critical questions surrounding the rollout of 5G, facial recognition for surveillance, automated cyber exploitation and defense, and autonomous weapons systems. A Japanese official responding to the CSET survey noted that the United States and its allies should adopt a citizen-centric AI strategy. Such citizen-centric strategies would seek to develop and deploy AI for the benefit of democratic societies, including strengthened data privacy standards and respect for civil liberties; economic empowerment of citizens within rules-based market economies; greater access to education, precision medicine, energy efficiency, and more inclusive social service provision.

The United States should lead a multilateral effort with allies and partners to set international rules of conduct for AI. This effort should build on and extend the OECD Principles on AI and the International Organization for Standardization working group initiatives on standards for data and AI safety and security. The United States and its allies could establish a standing platform to coordinate policies on standard-setting in multilateral fora. This is likely an area for productive dialogue, as partners are eager to coordinate policies and share best practices around norms and standards. In fact, all surveyed officials were extremely or very interested in this avenue for international collaboration.

Longer term, the United States and its allies should explore the conditions for a common AI market, including standards for testing, verification, and validation of AI technologies, as well as common practices for certifying companies that support liberal democratic values and privacy.87 This common market would create incentives for other countries to abide by these principles in the development and deployment of safe and reliable AI. As one EU representative observed, if the West could offer a viable way of doing AI that respects privacy and fundamental rights, developing (and democratic) countries would be more inclined to follow the Western model.

#### Solves democracy

Andrew Imbrie et al 20, Andrew Imbrie Ryan Fedasiuk Catherine Aiken Tarun Chhabra Husanjot Chahal. Center for Security and Emerging Technology (CSET) at Georgetown’s Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. February. "Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI" //pipk

How can the United States collaborate with allies and partners to shape the trajectory of AI in ways that will promote liberal democratic values and protect against authoritarian uses of this technology?

The evidence in this report suggests alliances are relevant to defending against Chinese and Russian efforts to wield AI for authoritarian ends, networking with partners to advance technological progress, and projecting shared democratic values in the age of AI.

Forging a democratic way of AI requires blending two strategic approaches: signaling and shaping.95 The United States needs to formulate policies that signal resolve to strategic competitors and reassurance to allies and partners. By pursuing the initiatives outlined in this report, the United States can communicate resolve through sensible policies, smart investments, and clarity about intentions. Equally important, the United States will need to deepen cooperation with allies and partners to shape the ecosystems for development and deployment of safe and reliable AI.

By coordinating with allies and partners to counter technology transfer, leverage hardware chokepoints, invest in privacy-preserving machine learning, share non-sensitive data sets, foster R&D collaboration, develop human capital, enhance interoperability, promote global norms and standards, and establish a digital infrastructure network, the United States and its allies can shape the global environment in ways that support democratic values. The stakes are clear, and the stage is set for the United States and its allies to rise to the challenge.

### 2AC---AI Solves Disinfo---Democracy I/L

#### AI solves disinformation

David Calvo et al 21, Project Lead, NATO ACT Innovation Hub. Johns Hopkins University: David Calvo, Ricky Cheng, Marc Helou, Nyeli Kratz, Claire Liddy, Jolie McDonnell, Tyler Shin. Imperial College London: Jasneet Taak Georgia Institute of Technology: Jack Crawford, Meredith Furbish, Marc Al Haj, Nico Luzum, Omar Webb Under the Supervision of: Lawrence Aronhime, Associate Teaching Professor, and Alexander Cocron, Lecturer, Johns Hopkins University Whiting School of Engineering. Nicholas Nelson, Principal Researcher, Georgia Tech Research Institute (GTRI); Senior Fellow for Emerging Tech & Policy at the Center for European Policy Analysis (CEPA). August 12. “Countering disinformation: Improving the Alliance’s digital resilience” <https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html> //pipk

The Alliance needs a broadly effective strategy to counter the evolving threat of disinformation. Artificial intelligence (AI) tools can help to identify and to slow the spread of false and harmful content while upholding the values of pluralistic and open societies.

Disinformation: not exactly new

False information and misleading narratives have been tools of conflict and statecraft since the fabled city of Troy fell to the ancient Greeks, and probably before. In the distant past, there were fabricated wooden horses, false witnesses, and faked plans. Today, we have fake news, false social media profiles, and fabricated narratives created to mislead—sometimes as part of coordinated cognitive warfare campaigns.

Countering cognitive warfare: awareness and resilience

Related Article : Countering cognitive warfare: awareness and resilience

Social media and the internet have enabled a disinformation revolution. We live in a world of low-cost digital instruments and media with radically expanded reach, scale, and impact. And the concern is that these easily accessible instruments are available not merely to state actors, but to non-state actors, private individuals, and everyone in between.

Social media and the internet have enabled a disinformation revolution that impacts state actors, non-state actors, private individuals, and everyone in between.

© Centre for Research and Evidence on Security Threats

Social media and the internet have enabled a disinformation revolution that impacts state actors, non-state actors, private individuals, and everyone in between. © Centre for Research and Evidence on Security Threats

Disinformation in the Western Balkans

Related Article : Disinformation in the Western Balkans

False messages and inflammatory narratives have made headlines in extreme cases, notably in the Western Balkans and in some Allied countries. Their more insidious danger is the damage they can do to citizens’ faith in the institutions of democratic governance and resources of public information and discussion. And recent years have seen growing political polarisation, historically low levels of trust in governing institutions, and instances of unrest and violence, aided in part by false information.

The "Lisa case": Germany as a target of Russian disinformation

Related Article : The "Lisa case": Germany as a target of Russian disinformation

NATO member countries maintain open civil communications systems, some with very high rates of social media and social messaging use. The pluralistic characters of their societies, while an advantage and source of strength, can at the same time provide opportunities for divisive or incendiary narratives to take hold. For many of these countries, resilient and protective regulatory structures are still in their infancy. The combination of these conditions makes the threat of disinformation of particular concern for the Alliance.

The focus on false facts

Global social media companies have taken up the challenge to mitigate false information on their platforms. Most employ in-house human fact checkers to monitor the dissemination of false information. Some rely on third-party human fact checking or moderating tools. Several popular platforms, including Facebook, YouTube, and Twitter provide their users with the option to report other users suspected of spreading false information, either knowingly or unknowingly. And in an effort to retroactively correct for the damage caused by false information, the vast majority of social media platforms have used the mass removal of content identified as harmful or misleading via these methods.

At best, this has proved to be too little, too late. At worst, it has led to accusations of censorship, and to the removal of information or opinions that later turned out to be credible or worthy of public discussion.

The problem of volume

There are nearly three billion monthly active users on Facebook alone, each one capable of posting something inflammatory online. Twitter has over 350 million active users, including prominent individuals, popular opinion leaders, and clever and resourceful influencers.

The current approach to counter disinformation relies mostly upon manual fact-checking, content removal, and damage-control. While human interventions may be useful in cases requiring nuanced understanding or cultural sensitivity, they are poorly matched to the large volumes of information created every day. It is unlikely that adding more personnel is a realistic option to proactively identify false or damaging content before it has the chance to spread widely. Human fact checking is, in itself, subject to error, misinterpretation, and bias.

Billions of monthly active users of social media are capable of posting something inflammatory online. This is an overwhelming amount of information for manual fact-checkers.

© The Globe and Mail

Billions of monthly active users of social media are capable of posting something inflammatory online. This is an overwhelming amount of information for manual fact-checkers. © The Globe and Mail

What goes viral?

“Falsehood flies and truth comes limping after it” wrote the satirist Jonathan Swift in the 17th Century. A recent MIT study found that on Twitter, false news items are much more likely to go viral, and regular users, not automated ‘bots,’ are responsible for re-sharing them. People also ‘retweet’ these false news items with sentiments of surprise and disgust. By contrast, true stories produce sentiments of sadness, anticipation, and trust (and are much less frequently shared).

This raises a potential opportunity: Should we focus not on facts, but on emotions instead? And could computers, not humans, be trained do so?

Don’t check facts, check emotions

Artificial intelligence-based sentiment analysis represents an entirely different approach to mitigating disinformation by training computers to identify messages and posts containing elements of surprise, disgust, and other emotional predictors. These are more likely to be associated with false information and to inflame the passions of social media users.

Natural language processing algorithms make it possible to identify linguistic indicators of the emotions in question. They avoid human fact checking altogether, reducing bias and cost, and increasing processing speeds. A student team at Johns Hopkins University has created a promising working prototype, and their teammates at the Georgia Institute of Technology and Imperial College London have developed feasibility assessments and potential regulatory approaches.

Don’t stop disinformation, slow it down

But once a highly viral (and likely false) message or post is identified, what to do? An analogy from the financial markets suggests a solution: an automated ‘circuit-breaker’ that temporarily suspends or slows the dissemination of emotionally charged content.

Stock markets avoid panic selling by temporarily suspending the trading of stocks that have declined by certain percentage thresholds. On the New York Stock Exchange, stocks that decline in price by over 7% are halted for 15 minutes in the first instance. The idea is to slow things down and let cooler heads prevail. Subsequent price declines can trigger additional trading suspensions.

The cooling effect of slowing things down can be significant. On a social messaging site, a message that doubles every 15 minutes can hypothetically reach one million views in five hours, and 16 million views in six hours. But if slowed to doubling every 30 minutes, it would reach only one thousand views in five hours and four thousand in six hours. Small differences in virality yield huge differences in exposure.

Such a mechanism would operate, not by preventing sharing, but by slowing engagement; for example, by imposing cool down periods between comments, or prompting users to consider possible consequences before resending a message. It builds on the central thesis in the Nobel Prize winner Daniel Kahneman’s book Thinking Fast and Slow. Slow thinking is rational and avoids the emotionality of fast reactions to surprising and shocking news or events.

This could reduce concerns of censorship or arbitrary limits upon the free flow of ideas. Messages and posts are not taken down or eliminated. They remain available for review and discussion, only at a slower pace. This mitigates the problem of who adjudicates ‘permissible speech’ and protects valuable freedoms of expression and public discourse. Such an approach could be implemented, via incentives or regulation, at various layers of the communication infrastructure: the source companies themselves, mediating gateways (or ‘middle-ware’ platforms), the message transport level (the communications ‘pipes’), or even at the device level (smartphone or tablet).

Considerations for the Alliance

Disinformation is one of several digital threats facing the Alliance. Recent information campaigns and cyberattacks have revealed that even technologically advanced member states must do more to prepare for current and emerging digital challenges. More progress is needed in establishing successful resilience mechanisms and regulatory frameworks.

Cyberattacks threaten even the most technologically advanced NATO members. More progress is needed in establishing successful resilience mechanisms and regulatory frameworks.

Cyberattacks threaten even the most technologically advanced NATO members. More progress is needed in establishing successful resilience mechanisms and regulatory frameworks.

Yet these threats appear to be increasing daily, leaving the Alliance with little time. Taking advantage of existing technologies (such as those mentioned above) and applying them in innovative ways should save both time and resources. Minimally invasive mitigation concepts, such as slowing—but not permanently deleting—potentially harmful social media messages and posts, may be the most promising first step to address the threat of disinformation. The Alliance can then spend more time on additional technology development and more comprehensive regulatory approaches in the future.

Historically, the resilience and strength of open and pluralistic societies has been in their ability to adapt innovatively to emerging challenges and circumstances. A foundational mechanism for this is the free flow of ideas and information, as well as the open and public discussion and examination of options, policies, and plans. Any solution to disinformation must protect this mechanism if we wish to keep this advantage. Moreover, the adoption of solutions by member states will rely upon the acceptance of their societies at large and is unlikely to succeed if internal constituencies consider themselves marginalised or excluded from the public dialogue.

NATO could endeavor to promote the adoption of such technology- and principles-based approaches while leaving member states to decide their own national digital security strategies. This would provide member state governments with the flexibility to implement mechanisms as they see fit, congruent with their local levels of social media adoption, popular expectations of free expression, and the realities of their civil communications infrastructures.

### 2AC---US-EU Relations Add-on

#### US-EU relations solve multiple existential risks

Bruce Stokes 20, fellow at the German Marshall Fund, a former international economics correspondent for the National Journal, a former senior transatlantic fellow at the German Marshall Fund and a former senior fellow at the Council on Foreign Relations. "Together or Alone? Choices and Strategies for Transatlantic Relations for 2021 and Beyond". October. <https://www.gmfus.org/sites/default/files/Task%2520Force%25202020_Oct_5_Final%2520%2528With%2520Footnotes%2529.pdf> //pipk

In 2021, the United States and the nations of Europe will face challenges that threaten their way of life: a catastrophic pandemic, a deep economic recession, accelerating climate change, a rising China, growing technological competition, and emerging security threats.

These challenges test our ability to deliver on our promise to safeguard and enhance the lives of our people. They confront the transatlantic community at a time when many citizens on both sides of the Atlantic continue to question whether their governments are able to deliver for them. These are issues that transcend national borders. They cannot be successfully dealt with alone. They can only be resolved through concerted, cooperative international action.

This Transatlantic Task Force report recommends concrete policy initiatives the United States and Europe can take together to manage our pressing shared problems. We make these recommendations, not because they will be easy to implement, but because they represent practical options to help address the key challenges we face.

Political change is underway on both sides of the Atlantic. In 2021, the United States may have a new president. The United Kingdom will formally leave the European single market, complicating transatlantic relations. And Germany will hold a national election and have new leadership by the fall.

But the ability of Europe and the United States to work together in the face of shared challenges faces an even more daunting test: public disenchantment with each other. Many Europeans, disillusioned with the United States and its leadership, desire greater economic, technological, and military autonomy. In the United States, supporters of President Donald Trump share his view that the United States has long been taken advantage of by its European allies.

The transatlantic relationship has weathered storms in the past. For more than seven decades, Europe and the United States have stood side by side in the face of threats to their wellbeing: during the Cold War, following 9/11, and once more in the aftermath of the 2009-2010 financial crisis. Our successful cooperation has been based on common interests and a shared set of democratic values that have led to greater security and prosperity for our people. But past performance is no assurance of future success.

In the face of existential challenges, such as climate change, pandemics, and competition from China, neither the United States nor its European partners can effectively act alone. Rather, these problems offer us an opportunity to find new ways to work together to build a better future for our people and the world. Our publics support such cooperative effort. Roughly six-in-ten Americans and Europeans believe that when dealing with major international issues their nation should take into account other countries’ interests, even if it means making compromises. In so doing, we can set an example for the world, laying the foundation for much broader cooperation among like-minded democracies that ultimately will be necessary to cope with what today are truly global challenges. In the process, we can transform the transatlantic relationship, assert U.S.-European leadership, affirm our citizens’ faith in our democratic values and each other, and demonstrate the ability of our democratic institutions to solve their people’s problems.

We understand that some of the initiatives we propose lack bipartisan support in the United States and may not be embraced by the next administration. Nor will they appeal to all Europeans. But several of them build on ideas and efforts already proposed by U.S. President Donald Trump, former U.S. Vice President Joe Biden and some European leaders. None of them are a one-year exercise. Meeting these new challenges will take an effort on the scale and duration of past alliance solidarity. The problems are clear, and their shared nature is self-evident. Now is not the time for more reflection and muddling through. Both sides of the Atlantic are facing very real threats to our way of life and concrete action is required to deal with these issues and preserve the democratic order that Americans and Europeans built together over the past seven decades.

The following recommendations reflect the deliberations of the co-chairs and the 14 American and European task force members, supplemented by interviews by the executive director with more than 150 European and American experts from diverse fields and countries. They are the sole responsibility of the executive director and the co-chairs; individual recommendations do not necessarily reflect the views of all task force members nor those who were interviewed, who are listed in the appendix.

### 2AC---US Key to Global Democracy

#### US key to global democracy---counterplan establishes safeguards for three pillars, civic organizations are key

Larry Diamond 21, Senior Fellow at the Hoover Institution and the Freeman Spogli Institute for International Studies at Stanford University. "A World Without American Democracy?". Foreign Affairs. July 2. https://www.foreignaffairs.com/articles/americas/2021-07-02/world-without-american-democracy

A prolonged global democratic recession has, in recent years, morphed into something even more troubling: the “third reverse wave” of democratic breakdowns that the political scientist Samuel Huntington warned could follow the remarkable burst of “third wave” democratic progress in the 1980s and the 1990s. Every year for the past 15 years, according to Freedom House, significantly more countries have seen declines in political rights and civil liberties than have seen gains. But since 2015, that already ominous trend has turned sharply worse: 2015–19 was the first five-year period since the beginning of the third wave in 1974 when more countries abandoned democracy—twelve—than transitioned to it—seven.

And the trend continues. Illiberal populist leaders are degrading democracy in countries including Brazil, India, Mexico, and Poland, and creeping authoritarianism has already moved Hungary, the Philippines, Turkey, and Venezuela out of the category of democracies altogether. In Georgia, the dominance of the Georgian Dream Party has led to the steady decline of electoral processes and a breakdown in the rule of law. In Myanmar, the military overthrew the elected government of Aung San Suu Kyi, ending an experiment in partial democracy. In El Salvador, president Nayib Bukele staged an executive coup by removing the attorney general and Supreme Court justices who were obstacles to his consolidation of power. In Peru, democracy hangs from a thread as the right-wing autocrat Keiko Fujimori advances vague claims of election fraud in a bid to overturn her narrow electoral defeat to left-wing opponent Pedro Castillo.

What is especially striking about this last case is that Fujimori’s gambit bears a grim resemblance to the lie perpetuated by former U.S. President Donald Trump and his followers about the 2020 presidential election. This is no coincidence. As the journalist and historian Anne Applebaum has observed, fictitious claims of fraud and “stop the steal” tactics are becoming a common means by which autocratic populists try to obstruct democracy. Such tactics have long been a source of instability in countries struggling to develop democracy. But the fact that the most recent iteration of the antidemocrat’s playbook draws heavily on precedents in the world’s most important and powerful democracy marks the start of a dangerous new era.

Today, the United States confronts a growing antidemocratic movement, not just from the ranks of fringe extremists but also from a substantial group of officeholders—a movement that is challenging the very foundations of electoral democracy. Should this effort succeed, the United States could become the first ever advanced industrial democracy to fail—that is, to no longer meet the minimum conditions for free and fair elections as political scientists and other scholars of democracy define them.

The failure of American democracy would be catastrophic not only for the United States; it would also have profound global consequences at a time when freedom and democracy are already under siege. As Huntington noted, the diffusion of democratic movements and ideas from one country to another has helped drive positive democratic change. Antidemocratic norms and practices can spread in a similar fashion—especially when they emanate from powerful countries. That is why the acceleration of a democratic recession into a democratic depression happened largely on Trump’s watch. And it is why no development would more gravely damage the global democratic cause than the democratic backsliding of its most important champion.

THE DEMOCRATIC TRIAD

A democratic system of government stands on three legs. The first leg is popular sovereignty—rule by the people. Democracy demands that people are able to choose and replace their leaders in regular, free, and fair elections; that all adult citizens are able to vote free from intimidation and obstruction; and that candidates and parties are free to compete and campaign. Crucially, elections must be administered impartially, so that valid ballots are counted accurately and power is granted to those who win.

Liberty is the second leg of liberal democracy. A fully democratic system provides strong protections for freedom of speech, the press, association, and assembly. It ensures that these rights are equally protected for all social groups. And it promotes a culture of mutual tolerance and respect for the rights of political opponents.

The third leg—the rule of law—defends and strengthens the other two. It ensures that democratic procedures are impartially enforced by an independent judiciary and other regulatory bodies that check the abuse of power. In most advanced democracies, excluding the United States, these instruments of accountability include national bodies to administer elections and to monitor corruption.

Trump was the first U.S. president to demonstrate contempt for all three legs of the triad of liberal democracy. He attacked the media as “fake news” and “absolute scum” and called for his election opponent to be “locked up.” He invited his followers to commit acts of violence against protesting opponents. Upon his defeat, he insisted that the election results were fraudulent and had to be overturned. Throughout his presidency, he waged war on an independent judiciary, the Federal Bureau of Investigation, his own attorney general, the Office of Government Ethics, the civil service, and a host of other actors who refused to bend to his political will or sought to enforce the rule of law.

The United States’ outsize importance will influence struggling democracies and embattled autocracies alike.

Many scholars of democracy perceived an unprecedented threat to U.S. democracy when Trump entered office in 2017 and feared grave assaults on the second and third legs of the democratic triad, in particular. This assessment was partially correct. Not since President Richard Nixon and rarely in U.S. history has there been such a determined effort to misuse and subvert administrative and rule-of-law institutions for nakedly political ends—but these attempts achieved only limited effect. The bulk of the press and the judiciary remained independent. The FBI avoided political capture. Outside the Republican Party and Trump’s own administration, freedom of speech thrived. From 2017 through 2020, liberty and the rule of law more or less held.

In three respects, however, most scholars misjudged the nature of the peril—and underestimated its gravity. First, many assumed that Trump himself constituted the biggest threat to U.S. democracy and that his defeat would lance the poisonous boil on the body politic. Second, with notable exceptions, including the Yale historian Timothy Snyder and the Carnegie Endowment scholar Rachel Kleinfeld, many underestimated the potential for violence on the part of Trump’s true-believing followers. And third, most underestimated the extent to which Trump would remake the Republican Party as an institution not only slavishly loyal to him but also hostile to democracy.

Fortunately, leading up to the 2020 election, democracy scholars and civic organizations correctly anticipated the threats to electoral integrity posed by zealous Trump partisans, as well as the staggering logistical challenges presented by the pandemic. As a result, they launched one of the most energetic civic campaigns in U.S. history to register an unprecedented number of voters, to give them safe and early access to the ballot, to ensure that local electoral administrations had the resources necessary to administer the vote, and to prepare to combat any potential efforts to overturn the legitimate results of the presidential election. The election was not a nightmare scenario, as some had feared. In fact, it proved to be one of the best-administered elections in U.S. history, leading election experts Nathaniel Persily and Charles Stewart III to call it a “miracle.”

IT COULD STILL HAPPEN HERE

Yet what followed was, in the words of Persily and Stewart, a “tragedy,” with “lies about vote fraud and the performance of the system [cementing] a perception among tens of millions of Americans that the election was ‘rigged.’” Such “manufactured distrust” has extended past the January 6 insurrection in Washington. Although President Joe Biden’s inauguration has deescalated imminent threats to civil liberties and the rule of law, the core element of electoral democracy—free and fair elections—is now under relentless partisan assault. Republican state legislatures are accelerating efforts to make it more difficult for African Americans, Latinos, and other Democratic-leaning constituencies to vote by passing laws that make it more difficult to vote by mail and to vote early, and that make it easier to purge voters from voting rolls. These changes are driven not by documented evidence of malfeasance associated with these practices but by deliberately false narratives about election fraud.

Now, the greatest threat to American democracy is posed by legislative initiatives seeking to subvert the independence of electoral administration, including the counting and certification of the vote. As the election law expert Richard Hasen has observed, “At stake is something I never expected to worry about in the United States: the integrity of the vote count.” A recent law passed in Georgia, for example, removes the secretary of state (currently Brad Raffensperger, who refused to manufacture the 11,780 votes Trump needed to win the state) as chair of the state Election Board and gives the state legislature—a highly partisan institution—the ability to name the new chair. Representatives in Michigan have politicized the Board of State Canvassers, which certifies election results, by replacing a Republican who voted to certify Biden’s election victory with a movement conservative. In Michigan and in Nevada, Trump loyalists are seeking to consolidate control over election supervision by running candidates for secretary of state—giving them the authority to preside over election administration and the tools to try to block Democratic votes. And at the federal level, Republicans could take back control of the House of Representatives (helped by their unilateral ability to redraw 187 congressional districts following the most recent census) and use their majority to manipulate the 2024 presidential results in their favor—especially if the 2024 election resembles 2020, when Democrats won a decisive popular vote victory but relied on narrow margins in a handful of states for an Electoral College majority.

Once a political system loses bipartisan consensus respecting the rules of the democratic game, it can be a short slide to autocracy. The world has watched this happen in Hungary, Turkey, and Venezuela. It is not inconceivable that it could happen in the United States.

THE GATHERING STORM

To warn of the failure of American democracy is not hyperbole or simply a slogan meant to motivate action. Political scientists may differ on the minimum conditions for democracy, but they agree on this: a country cannot be considered a democracy if it does not broadly ensure the neutral and fair administration of elections. If the outcome of a major national election in the United States were to be determined by fraudulent exclusion or the manipulation of votes, the country would cease to be a democracy, no matter how much freedom of expression might survive (for a time).

More than 100 prominent democracy scholars recently warned in a collective statement that Republican assaults on electoral integrity could bring about the demise of U.S. democracy. They appealed to Congress to pass the John Lewis Voting Rights Act and to adopt other measures to “ensure the sanctity and independence of election administration.” But with broad national legislation to ban partisan gerrymandering and strengthen voting standards unlikely in the near term, it will also be up to civil society to defend American democracy.

That defense is made more urgent by the gathering storm of democratic backsliding around the world. The United States’ outsize importance as a source of political diffusion, for good or ill, makes it an example that will influence struggling democracies and embattled autocracies alike. Both in backsliding democracies such as the Philippines and Poland and in deepening autocracies such as Turkey and Venezuela, Trump’s mantra of “fake news” emboldened strongman leaders in their assaults on the media. If the United States winds up disfiguring its democracy by politicizing electoral administration and suppressing minority votes, autocrats will gleefully seize upon the American precedent as justification for their methods of blocking democratic change. And in declining democracies, politically vulnerable incumbents will embrace similar methods of violating electoral integrity in order to hang on to power.

In short, what happens to democracy in the United States is likely to determine the fate of democracy around the world: whether this third wave of democratic reversals is turned back or gains horrific new momentum.

### 2AC---AT: Decline Inevitable

#### Decline reversible

Nancy Bermeo 18, American political scientist, and senior research fellow at Nuffield College, University of Oxford. "Reflections: Can American Democracy Still Be Saved?" <https://journals.sagepub.com/doi/10.1177/0002716218818083?icid=int.sj-related-articles.similar-articles.7> //pipk

This article reflects on whether the erosion of democracy in the contemporary United States can be halted. Using the cases and conclusions from McCoy and Somer’s eleven country collective project, it argues that democracy’s decline is not inevitable. A case for cautious optimism emerges from analyzing the coalitions around democracy’s disassemblers and democracy’s defenders. The actors disassembling democracy have activated cleavages and adopted a style of rule that exacerbates fault-lines on the Right. The actors defending democracy have thus far done what’s needed to eventually build the sort of winning coalition that has proven successful elsewhere. Creating broad, cross-class networks, mobilizing peaceful protest, and drawing on mass values that are still supportive of democracy bolster the likelihood of successful defense.

### 2AC---DPT True

#### The most exhaustive quantitative study finds DPT to be true.

Imai '21 - Professor of Government and of Statistics at Harvard University [Kosuke and James Lo, "Robustness of Empirical Evidence for the Democratic Peace: A Nonparametric Sensitivity Analysis," International Organization, Vol 75, Issue 3]

How should we resolve this empirical debate regarding the democratic peace?Footnote9 Unfortunately, in the absence of randomized experiments, we can never completely rule out the possible existence of confounding biases that arise from omitted variables. While scholars in this literature have exclusively relied on parametric regression models, this approach requires strong assumptions, namely that the model accurately characterizes the true data-generating process (correct set of variables, right functional form, valid distributional assumption, etc.). Given that these assumptions may not be verifiable from observed data, it is no surprise that various scholars advocate different regression models with diverging sets of variables, resulting in contradictory findings. The difficulty of adjudicating between these alternative modeling approaches has led to the ongoing controversy in the empirical democratic peace literature.

We propose an alternative approach based on nonparametric sensitivity analysis to formally assess the robustness of the empirical evidence.Footnote10 Specifically, we quantify the strength of confounding relationships that could explain away the observed association between democracy and peace. That is, we compute the precise level of unobserved confounding needed to render the observed association between democracy and conflict spurious. The idea is that although not all correlations imply causation, a very strong correlation suggests it. Unlike the parametric regression modeling approach prevalent in the literature, the proposed nonparametric sensitivity approach directly addresses the existence of unobserved confounders without assuming a particular regression model.Footnote11 Although one can never know with certainty from observational data whether democracy causes peace, this nonparametric sensitivity analysis can formally assess the robustness of empirical evidence for the democratic peace.

Our analysis applies the nonparametric sensitivity analysis method originally developed by Cornfield and colleagues, who were concerned with the robustness of the positive association between cigarette smoking and lung cancer in the potential presence of unobserved confounders.Footnote12 The study of the causal relationship between smoking and lung cancer closely parallels the dispute on the democratic peace. In both cases, randomized experiments cannot be conducted for ethical and logistical reasons, and critics contend that the observed association suffers from confounding biases. While no definitive conclusion can be drawn from observational data, Cornfield and colleagues argue that no existing confounder can explain the strong association between smoking and cancer and therefore this relationship is likely to be causal. Their conclusion is worth quoting here:

Cigarette smokers have a ninefold greater risk of developing lung cancer than nonsmokers, while over-two-pack-a-day smokers have at least a 60-fold greater risk. Any characteristic proposed as a measure of the postulated cause common to both smoking status and lung-cancer risk must therefore be at least nine-fold more prevalent among cigarette smokers than among nonsmokers and at least 60-fold more prevalent among two-pack-a-day smokers. No such characteristic has yet been produced despite diligent search.Footnote13

Our application of nonparametric sensitivity analysis to the democratic peace yields striking results. Depending on the definition of democracy, we find that a confounder must be at least forty-seven times more prevalent in democratic dyads than in other types of dyads. Thus, any potential confounder that could explain the democratic peace would have to be at least five times as prevalent as a similar confounder for smoking and lung cancer. In other words, according to our analysis, the positive association between democracy and peace is much more robust than that between smoking and lung cancer.

#### Democratic peace is true

Havard Hegre et al 19, Department of Peace and Conflict Research, Uppsala University. Journal of Conflict Resolution, Vol 64, Issue 1, 2020. "Civil Society and the Democratic Peace" <https://journals.sagepub.com/doi/full/10.1177/0022002719850620> //pipk

We theorize that three distinct structures of democratic constraint explain why more democratic dyads do not engage in military conflict with each other. We build on earlier theories that focused on electoral and horizontal accountability. We add a new dimension—the social accountability provided by an active civil society. Using several new measures from the Varieties of Democracy (V-Dem) data set, we stringently test these explanations. We find social accountability to be the strongest and most consistent predictor of nonbelligerence in dyads, that horizontal accountability is still important, but that the independent role of electoral accountability has been somewhat overstated. However, we do find that social and electoral accountability work strongly together, to make for an even greater effect. The finding is robust to a range of specifications and in the face of controls for contending theories that challenge the democratic peace (e.g., the capitalist and territorial peace theories).

The democratic peace has proved to be one of the most influential and durable findings in the history of international relations, if not political science as a whole. As with all influential findings, alternatives have been posed, for example, the “capitalist peace” (Gartzke 2007; Mousseau 2000, 2009, 2013), the “territorial peace” (Gibler 2012), or “political similarity” (Bennett 2006; Raknerud and Hegre 1997; Peceny, Beer, and Sanchez-Terry 2002; Werner 2000). Beyond such empirical challenges, the finding has also been criticized for not providing a fully convincing causal logic that explains the empirical finding (Rosato 2003). This puzzle of what makes democracies less likely to engage in conflict with other democracies still remains subject to a lively and inconclusive debate (Hegre 2014). Our purpose here is to use the new Varieties of Democracy (V-Dem) data, with its ability to more precisely disaggregate the components of democracy, to reconsider its causal logic in a more precise fashion and with a fresh perspective.

We advance the debate by arguing that different forms of constraint on power holders help to explain why democratic dyads are less likely to engage in conflict. To date, the greatest attention has been focused on what we term electoral and horizontal accountability. Electoral accountability (sometimes referred to as vertical accountability) functions because elected politicians try to avoid alienating voters in anticipation of the next round of elections. Horizontal accountability operates through the ability of other branches of government and state institutions to check the power of the executive. We build on previous work that showed that greater electoral participation (Reiter and Tillman 2002; Clark and Nordstrom 2005; Bueno de Mesquita et al. 1999) and greater horizontal constraints on the executive (Reiter and Tillman 2002; Clark and Nordstrom 2005; Choi 2010) work to reduce conflict. An important part of our contribution is to add a new dimension—social accountability. It is provided by organized actors in civil society that have the ability to inflict audience costs on the executive in-between elections and to mobilize in support of opponents during elections.

We also highlight a new measurement tool for capturing democracy as an aggregate and in its component parts in new and potentially fruitful ways. Whereas the vast majority of studies have relied on Polity to capture the degree of democracy among states, we use the V-Dem data, which have both better concept-measurement consistency and also allow us, because of the ability to disaggregate components of democracy, to directly test the different forms of constraint we discussed above. Our sample includes observations from 173 countries across the globe from 1900 to 2010. We test whether these three different forms of accountability—(1) horizontal, (2) electoral, and (3) social—restrain democracies from fighting with each other. When pitting the three mechanisms of accountability directly against each other, we find the weakest support for the form that has received the greatest attention in the literature—electoral. However, its effect becomes salient when it is combined with social accountability between elections. The democratic peace effect thus seems less a product of simple electoral constraint than on the ability of civil society, as well as other state actors, to constrain the incumbent. To our knowledge, this is the first time that anyone has tested the impact of civil society engagement on conflict behavior. In an Online Supplementary File (henceforth SF),1 we demonstrate that our main findings are robust in the face of contending theories and alternate specifications of our tests.

#### Data supporting DPT is stronger than smoking causes lung cancer---they use regression analysis, we use nonparametric sensitivity analysis, we are not the same

Kosuke Imai and James Lo 21, Professor of Government and Statistics, Harvard. "Robustness of Empirical Evidence for the Democratic Peace: A Nonparametric Sensitivity Analysis" International Organization, Volume 75, Issue 3. April 5.. <https://www.cambridge.org/core/journals/international-organization/article/abs/robustness-of-empirical-evidence-for-the-democratic-peace-a-nonparametric-sensitivity-analysis/66A4FFF9F79348AB926284EC32EC11AB> //pipk

The democratic peace—the idea that democracies rarely fight one another—has been called “the closest thing we have to an empirical law in the study of international relations.” Yet, some contend that this relationship is spurious and suggest alternative explanations. Unfortunately, in the absence of randomized experiments, we can never rule out the possible existence of such confounding biases. Rather than commonly used regression-based approaches, we apply a nonparametric sensitivity analysis. We show that overturning the negative association between democracy and conflict would require a confounder that is forty-seven times more prevalent in democratic dyads than in other dyads. To put this number in context, the relationship between democracy and peace is at least five times as robust as that between smoking and lung cancer. To explain away the democratic peace, therefore, scholars would have to find far more powerful confounders than those already identified in the literature.

The proposition that democratic states do not fight interstate wars against each other is one of the most enduring and influential ideas in international relations. The idea is theoretically rooted in the work of Immanuel Kant, who argued that interactions between states with a republican form of government give “a favorable prospect for the desired consequence, i.e., perpetual peace.”1 This has led to a large literature empirically documenting a negative association between democracy and conflict,2 leading one scholar to comment that the democratic peace is “the closest thing we have to an empirical law in the study of international relations.”3

Despite the law-like nature of this association, no scholarly consensus has emerged on whether the observed association reflects a causal relationship or a spurious correlation. According to a recent survey, more than 30 percent of international relations scholars disagree with the democratic peace theory.4 In particular, skeptics have challenged the democratic peace by arguing that alliance structures from the Cold War,5 capitalism,6 and contract-intensive economies7 confound the observed association. These authors find that adding certain confounding variables to regression models eliminates the statistical significance of the estimated coefficient for the joint democracy variable.8

How should we resolve this empirical debate regarding the democratic peace?9 Unfortunately, in the absence of randomized experiments, we can never completely rule out the possible existence of confounding biases that arise from omitted variables. While scholars in this literature have exclusively relied on parametric regression models, this approach requires strong assumptions, namely that the model accurately characterizes the true data-generating process (correct set of variables, right functional form, valid distributional assumption, etc.). Given that these assumptions may not be verifiable from observed data, it is no surprise that various scholars advocate different regression models with diverging sets of variables, resulting in contradictory findings. The difficulty of adjudicating between these alternative modeling approaches has led to the ongoing controversy in the empirical democratic peace literature.

We propose an alternative approach based on nonparametric sensitivity analysis to formally assess the robustness of the empirical evidence.10 Specifically, we quantify the strength of confounding relationships that could explain away the observed association between democracy and peace. That is, we compute the precise level of unobserved confounding needed to render the observed association between democracy and conflict spurious. The idea is that although not all correlations imply causation, a very strong correlation suggests it. Unlike the parametric regression modeling approach prevalent in the literature, the proposed nonparametric sensitivity approach directly addresses the existence of unobserved confounders without assuming a particular regression model.11 Although one can never know with certainty from observational data whether democracy causes peace, this nonparametric sensitivity analysis can formally assess the robustness of empirical evidence for the democratic peace.

Our analysis applies the nonparametric sensitivity analysis method originally developed by Cornfield and colleagues, who were concerned with the robustness of the positive association between cigarette smoking and lung cancer in the potential presence of unobserved confounders.12 The study of the causal relationship between smoking and lung cancer closely parallels the dispute on the democratic peace. In both cases, randomized experiments cannot be conducted for ethical and logistical reasons, and critics contend that the observed association suffers from confounding biases. While no definitive conclusion can be drawn from observational data, Cornfield and colleagues argue that no existing confounder can explain the strong association between smoking and cancer and therefore this relationship is likely to be causal. Their conclusion is worth quoting here: Cigarette smokers have a ninefold greater risk of developing lung cancer than nonsmokers, while over-two-pack-a-day smokers have at least a 60-fold greater risk. Any characteristic proposed as a measure of the postulated cause common to both smoking status and lung-cancer risk must therefore be at least nine-fold more prevalent among cigarette smokers than among nonsmokers and at least 60-fold more prevalent among two-pack-a-day smokers. No such characteristic has yet been produced despite diligent search.13

Our application of nonparametric sensitivity analysis to the democratic peace yields striking results. Depending on the definition of democracy, we find that a confounder must be at least forty-seven times more prevalent in democratic dyads than in other types of dyads. Thus, any potential confounder that could explain the democratic peace would have to be at least five times as prevalent as a similar confounder for smoking and lung cancer. In other words, according to our analysis, the positive association between democracy and peace is much more robust than that between smoking and lung cancer.

While no such confounder has yet been found for the relationship between smoking and lung cancer, we examine whether the confounders identified in the democratic peace literature meet the conditions of nonparametric sensitivity analysis. For example, we consider a set of economic confounders proposed by Gartzke who argues that the democratic peace can be explained by capitalism.14 We also consider other confounders, such as military alliances.15 Overall, our findings imply that for a potential confounder to explain away the democratic peace, it must be much more strongly associated with regime types and conflicts than the confounders that have been proposed to date. This finding again demonstrates the robustness of empirical evidence for the democratic peace.

Finally, we believe that a nonparametric sensitivity analysis, such as the one we use here, can play an important role in international relations research, where the threat of omitted variable bias is almost always present. Although sensitivity analysis has been applied in international relations, almost all such applications have been based on parametric regression models. In the democratic peace literature, Kadera and Mitchell conduct a parametric sensitivity analysis in the spirit of Leamer.16 In addition, Chaudoin, Hays, and Hicks apply a parametric sensitivity analysis of Altonji, Elder, and Taber to the effects of the GATT/WTO, whereas Hegre and Sambanis use the method of Sala-i-Martin to examine the sensitivity of empirical results on civil war onset.17 The only exception we found is Davis and Shirato, who use a nonparametric sensitivity analysis to assess the robustness of their findings to possible sample selection bias.18 Unlike parametric approaches, nonparametric sensitivity analyses avoid modeling assumptions and hence offer a robust method to examine the strength of empirical conclusions.

### 1AR---Imai

#### **Prefer our evidence that outlines statistical methods from a peer reviewed article in a top IR journal over their cards that come from an unsubmitted working paper. Imai found that the relationship between democracy and peace is five times stronger than the relationship between smoking and lung cancer.**

#### Their randomized studies don’t cut it

Imai '21 - Professor of Government and of Statistics at Harvard University [Kosuke and James Lo, "Robustness of Empirical Evidence for the Democratic Peace: A Nonparametric Sensitivity Analysis," International Organization, Vol 75, Issue 3]

Unobserved confounding in observational research is one of the most fundamental methodological problems in social science. Although the randomization of treatments enables the identification of causal effects, such randomization is rarely feasible in many areas of social science, including political science. In such circumstances, different assumptions can yield conflicting results and yet it is impossible to assess the validity of competing assumptions. As a result, scholarly debates often end up in a scientific deadlock in which neither side is able to provide convincing evidence.

We believe that sensitivity analysis can play an essential role in making scientific progress in these difficult situations. While it cannot draw a definitive conclusion about causal relationships, sensitivity analysis allows researchers to evaluate the robustness of empirical findings by quantifying the minimum strength of unobserved confounding that must exist to explain away an observed association. An open-source software package, Evalue, is available for implementing the sensitivity analysis used here.Footnote58

### 2AC---Nigeria

#### Authoritarian countries have elections too; they have zero reverse causal ev.

#### A war caused by an authoritarian country triggers more instability.

Dutton '3/29 [Jack, "AfDB president: Ukraine war could trigger a food crisis in Africa," https://www.aljazeera.com/features/2022/3/29/afdb-president-ukraine-could-trigger-a-food-crisis-in-africa]

Effect of Ukraine war on Africa

Now, in his current role as the president of the African Development Bank, the continent’s largest multilateral lender, Adesina is trying to avert a food crisis on a larger scale. As the war between Russia and Ukraine draws into its second month, natural gas, wheat and fertiliser prices have skyrocketed.

Together Russia and Ukraine produce more than a quarter of global wheat exports, and Africa is heavily dependent on both countries. Wheat imports make up 90 percent of Africa’s $4bn trade with Russia and almost half of the continent’s $4.5bn trade with Ukraine, according to AfDB.

“One-third of the cereal supply of East Africa comes from those two countries, and Egypt is badly affected. So is Algeria and Morocco, Somalia and several other countries. So, if we don’t manage this very quickly, it will actually destabilise the continent,” Adesina said.

He said the war would affect Africa’s economy in a few major ways. Already, it has roiled financial markets, causing sky-high interest rates. “You begin to see what has happened also in terms of the yields for euro bonds that are posted by African countries. The spreads are very, very high as a result of this,” he said.

But perhaps just as important, commodity prices are on the increase, including that of wheat which has “gone up by 64 percent globally”, the same price around the 2008 global food crisis, he said.

Fertilisers, a key component of the agribusiness sector, have also been affected, and the bank chief knows that that could spell disaster.

“The price of urea has gone up by 300 percent. All of that is saying, that it’s [the war] driving inflation in Africa, and it could — if not quickly well-managed — trigger a food crisis in Africa,” Adesina said.

But perhaps just as important, commodity prices are on the increase, including that of wheat which has “gone up by 64 percent globally”, the same price around the 2008 global food crisis, he said.

Fertilisers, a key component of the agribusiness sector, have also been affected, and the bank chief knows that that could spell disaster.

“The price of urea has gone up by 300 percent. All of that is saying, that it’s [the war] driving inflation in Africa, and it could — if not quickly well-managed — trigger a food crisis in Africa,” Adesina said.

#### Election costs decreasing because of democracy.

Dazang '22 [Nick, 1/17/2022, "Understanding the high cost of elections," <https://guardian.ng/opinion/understanding-the-high-cost-of-elections/>]

\*INEC: Nigeria’s Independent National Electoral Commission

Ultimately, the cost of elections will come down if there is trust between stakeholders and INEC. Trust has to be earned by INEC by dint of transparency, impartiality, fairness and conducting excellent elections. Once elections are consistently adjudged to be superlative, they will become routine and we do not, in that context, need to emboss our “sensitive” materials with expensive security features or colour-code them. The ball is in INEC’s court.

### 1AR---Boko Haram

#### Their card is nine pages long and highlighted word salad – no one would sell Boko Haram nukes; unless they were the autocrats in charge of Nigeria. Doesn’t matter, because they’re wrecked.

Al Jazeera '3/24 ["Nigeria: 7,000 Boko Haram, other fighters surrender in a week," https://www.aljazeera.com/news/2022/3/24/nigeria-7000-boko-haram-other-terrorists-surrender-in-a-week]

Some 7,000 members of the Islamic State West Africa Province (ISWAP) and Boko Haram have surrendered in northeast Nigeria in the past week, according to local media reports.

On Wednesday, the News Agency of Nigeria quoted Major General Christopher Musa, a top commander in the region, as saying that an onslaught targeting ISWAP and Boko Haram fighters has continued to record significant success.

Musa said at least 7,000 Boko Haram and ISWAP members surrendered in the last week during the operations.

“This is evident as thousands of the insurgents comprising combatants, non-combatants, foot soldiers, alongside their families, continued to lay down their arms in different parts of Borno to accept peace,” he said.

The surrendering fighters and their families are expected to be profiled by the Nigerian army and other stakeholders before they undergo rehabilitation processes, the general added.

### 2AC---Warming

#### They are reading propaganda and utterly wrong about authoritarianism.

Butler '21 - history graduate and postgraduate student of International Relations at Leeds University [Alexander, 7/30/21, "Authoritarianism Can’t Beat Climate Change," https://thediplomat.com/2021/07/authoritarianism-cant-beat-climate-change/]

In some commentaries, authoritarianism and one-party rule, particularly China’s model of governance, is often portrayed as a magic bullet solution to the ostensible impending doom of climate change. In lieu of impotent governance, electoral cycles, short term policies, and hot-air promises of economic and environmental solutions, top-down authoritarian governance is touted as possessing the ability to implement the prudent and long-term policy capable of mitigating the worst effects of climate change.

This type of rhetoric is especially salient in authoritarian state-owned media around the world. Liberal democracies and the West, in particular, are portrayed as decadent, inefficient, dysfunctional, and archaic. Western governance models are seen as unable to meet the needs of the 21st century; they are ill-equipped to meet the social and economic needs of a growing population while mitigating the worst effects of climate change. Chinese state news agency Xinhua recently wrote of the United States’ “four deficits in climate action,” detailing the way in which inconsistency and “flip-flopping” has been the hallmark of U.S. climate policy. This view was further reaffirmed with the dramatic reversal of the Biden administration in re-joining the 2015 Paris Agreement after Donald Trump’s tumultuous exit in 2016. How are we to rely on capricious democracies when dealing with such a time-sensitive issue? Instead, China’s leadership is supposed to offer a decisive system of governance that is committed to “harmony between man and nature” and “green development.”

Indeed, these ideals are now enshrined in China’s Belt and Road Initiative (BRI). As Xi Jinping stated at the Leaders Climate Summit: “China has made ecological cooperation a key part of Belt and Road cooperation.” However, authoritarian state planning and top-down policies such as the BRI are not as omnipotent as often perceived. There is ample evidence to suggest the BRI is a fragmented, poorly planned, and ill-received initiative. In fact, the policy suffers from what some scholars have termed “fragmented authoritarianism.” BRI planning documents lack definition, are extremely “loose,” and BRI implementation is incredibly uncoordinated, with competing state agencies interpreting the vague rhetoric of the BRI for their own interests, often undermining the Party’s diplomatic objectives. Thus, if the BRI is to be understood as the ne plus ultra of authoritarian governments’ technocratic capability to implement policy decisively and successfully, it is not a very convincing one.

Overzealous enthusiasm for authoritarianism’s ostensible capacity to mitigate anthropogenic climate change also overlooks the importance of bottom-up and grassroots campaigns in stimulating public discussion and achieving climate justice and protection. Indeed, without the cumulative checks-and-balances of investigative journalism, activists, public figures, and NGOs, authoritarian governments do not face the same pressures or incentives familiar to democratic governments.

Civil society provides the impetus for climate policy. For example, the landmark 2013 Urgenda Foundation v. State of the Netherlands case was a legal battle between a climate activist group and their respective government. The activists successfully sued the Dutch state on the grounds of violating the European Convention on Human Rights for failing to implement policy that would ensure sufficient reductions of greenhouse gas emissions. Their success galvanized global civil society, and similar cases were heard in countries such as New Zealand, Ireland, Norway, Belgium, the United Kingdom, Germany, France, and Switzerland.

Advocates of the authoritarian model also overlook the agency that various sub-state and non-state actors possess in the mitigation of climate change. As perturbing as Trump’s exit from the 2015 Paris Agreement was, we also witnessed the collective agency of relatively autonomous cities in reaffirming their commitments to the Paris Agreement. Mayors from Los Angeles to New York City were animated in their objective of realizing the goals of the Paris Agreement, no matter what choices Washington made.

Without freedom of expression or freedom of the press, an active civil society cannot flourish, and meaningful debate regarding climate change remains stagnant and controlled by censorship. That was the case with the Chinese schoolgirl who was inspired by the global “Fridays for Future” campaign: Ou Hongyi’s protests were swiftly suppressed when told she could not return to school unless she “ditched” her climate activism.

If indeed there does exist a pathway out of global climate governance gridlock, the answer does not lie at the feet of authoritarian monoliths. Regardless of the inertia of authoritarian policy and the lack of civil society, an unwavering confidence in authoritarianism also overlooks how integral greenhouse gas-intensive industry is to performance legitimacy. Without electoral legitimacy, a sudden and decisive break away from this model of economic growth could jeopardize the credibility of one-party rule. This is a prospect most authoritarian leaders would wish to avoid.

Instead, we must look elsewhere for solutions. Most importantly, in addition to effective policy, the encouragement of transparent policy decisions, freedom of expression and freedom of the press are all absolutely fundamental to mitigating the worst effects of climate change.

### 2AC---AT: Lu

#### Lu is a K of neolib, which they don’t solve – concluding paragraph of the intro.

Dr. Chien-Yi Lu 21, PhD and MA in Government from the University of Texas, Austin, Visiting Scholar at Harvard University, Associate Research Fellow at the Institute of European and American Studies of Academia Sinica, Surviving Democracy: Mitigating Climate Change in a Neoliberalized World, Paperback Edition, 12/13/2021, p. 9

Where democracy remains trapped in its neoliberalized form—“more rather than less democracy”—is a guarantee for annihilation. Embracing authoritarianism, however, does not yield a different result for reasons that Passmore, Paehlke, Dryzek, and Stehr have explained. The only options left, therefore, are to sort out how democracy became neoliberalized, the mechanisms through which it took place, and to devise ways to bypass neoliberal controls in practicing democracy so that effective climate mitigation becomes possible and survival becomes attainable, even for the non-rich and non-powerful. The next chapter traces the neoliberalization of democracy to the Keynes-Hayek “debate,” demonstrating that the decadence of democracy was the intended consequence of a painstakingly designed economic-political order rather than the mere sum of mindlessness and sloppiness scattered here and there.

#### Voting negative is a vote for Putinism.

Hamid '22 - Senior fellow at the Brookings Institution, and assistant research professor of Islamic studies at Fuller Seminary [Shadi, 3/6/22, "There Are Many Things Worse Than American Power," https://www.theatlantic.com/ideas/archive/2022/03/putin-kremlin-imperialism-ukraine-american-power/624180/]

If there was any doubt before, the answer is now clear. Vladimir Putin is showing that a world without American power—or, for that matter, Western power—is not a better world.

For the generation of Americans who came of age in the shadow of the September 11 attacks, the world America had made came with a question mark. Their formative experiences were the ones in which American power had been used for ill, in Iraq and Afghanistan. In the Middle East more broadly, and for much longer, the United States had built a security architecture around some of the world’s most repressive regimes. For those on the left, this was nothing new, and it was all too obvious. I spent my college years reading Noam Chomsky and other leftist critics of U.S. foreign policy, and they weren’t entirely wrong. On balance, the U.S. may have been a force for good, but in particular regions and at particular times, it had been anything but.

Blaming America first became all too easy. After September 11, U.S. power was as overwhelming as it was uncontested. That it was squandered on two endless wars made it convenient to focus on America’s sins, while underplaying Russia’s and China’s growing ambitions.

For his part, Putin understood well that the balance of power was shifting. Knowing what he knew, the Russian president wasn’t necessarily “irrational” in deciding to invade Ukraine. He had good reason to think that he could get away with it. After all, he had gotten away with quite a lot for nearly 15 years, ever since the Russian war against Georgia in 2008, when George W. Bush was still president. Then he annexed Crimea in 2014 and intervened brutally in Syria in 2015. Each time, in an understandable desire to avoid an escalatory spiral with Russia, the United States held back and tried not to do anything that might provoke Putin. Meanwhile, Europe became more and more dependent on Russian energy; Germany, for example, was importing 55 percent of its natural gas from Russia. Just three weeks ago, it was possible for Der Spiegel to declare that most Germans thought “peace with Russia is the only thing that matters.”

The narrative of a feckless and divided West solidified for years. We, as Americans, were feeling unsure of ourselves, so it was only reasonable that Putin would feel it too. In such a context, and after four years of Donald Trump and the domestic turmoil that he wrought, it was tempting to valorize “restraint” and limited engagements abroad. Worried about imperial overreach, most of the American left opposed direct U.S. military action against Bashar al-Assad’s regime in the early 2010s, even though it was Russian and Iranian intervention on behalf of Syria’s dictator that bore the marks of a real imperial enterprise, not just an imagined one.

Russia’s unprovoked attack on a sovereign nation, in Europe no less, has put matters back in their proper framing. The question of whether the United States is a uniquely malevolent force in global politics has been resolved. In the span of a few days, skeptics of American power have gotten a taste of what a world where America grows weak and Russia grows strong looks like. Of course, there are still holdouts who insist on seeing the United States as the provocateur. In its only public statement on Ukraine, the Democratic Socialists of America condemned Russia’s invasion but also called for “the U.S. to withdraw from NATO and to end the imperialist expansionism that set the stage for this conflict.” This is an odd statement considering that Russia, rather than the United States, has been the world’s most unabashedly imperialist force for the past three decades. But many on the anti-imperialist left aren’t really anti-imperialist; they just have an instinctive aversion to American power.

America’s low opinion of its own capacity for good—and the resulting desire to retreat or disengage—hasn’t just been a preoccupation of the far left. The crisis of confidence has been pervasive, spreading to the halls of power and even President Barack Obama, whose memorable mantra was “Don’t do stupid shit.” Instead of thinking about what we could do, or what we could do better, Obama was more interested in a self-limiting principle. For their part, European powers—content to bask under their U.S. security umbrella—could afford to believe in fantasies of perpetual peace. Europe’s gentleness and lethargy—coaxing Germany to commit even 2 percent of its GDP to defense seemed impossible—became something of a joke. One popular Twitter account, @ISEUConcerned, devoted itself to mocking the European Union’s propensity to express “concern,” but do little else, whenever something bad happened.

Suddenly, the EU has been aroused from its slumber, and the parody account was rendered temporarily speechless. This is no longer tepid concern, but righteous fury. Member states announced that they would send anti-tank weapons to Ukraine. Germany, for the first time, said that it would ramp up its military budget to 100 billion euros. On the economic front, the EU announced some of the toughest sanctions in history. My podcast co-host, Damir Marusic, an Atlantic Council senior fellow, likened it to a “holy war,” European-style.

Sometimes, unusual and extreme events mark the separation between old and new ways of thinking and being. This week, the Berlin-based journalist Elizabeth Zerofsky remarked that the current moment reminded her of the memoir The World of Yesterday, written by the Austrian novelist Stefan Zweig as World War II loomed. In it, he recalls the twilight of the Austro-Hungarian Empire with an almost naive fondness. On the first day of the Ukraine invasion, I happened to be speaking to a group of college students who had no memory of September 11. I told them that they may be living in history. Those students, like all of us, are bearing witness to one of those rare events that recast how individuals and nations alike view the world they inhabit.

The coming weeks, months, and years are likely to be as fascinating as they are terrifying. In a sense, we knew that a great confrontation was coming, even if we hadn’t quite envisioned its precise contours. At the start of his presidency, Joe Biden declared that the battle between democracies and autocracies would be the defining struggle of our time. This was grandiose rhetoric, but was it more than that? What does it actually mean to fight such a battle?

In any number of ways, Russia’s aggression has underscored why Biden was right and why authoritarians—and the authoritarian idea itself—are such a threat to peace and stability. Russia invaded Ukraine, a democracy, because of the recklessness and domination of one man, Vladimir Putin. The countries that have rallied most enthusiastically behind Ukraine have almost uniformly been democracies, chief among them the United States. America is lousy, disappointing, and maddeningly hypocritical in its conduct abroad, but the notion of any moral equivalence between the United States and Putin’s Russia has been rendered laughable. And if there is such a thing as a better world, then anti-imperialists may find themselves in the odd position of hoping and praying for the health and longevity of not just the West but of Western power.

#### No statistical relationship between democracy and the environment.

Midlarsky 2018 - Rutgers University Moses and Annuta Back Professor of Political Science   
Manus, "Democracy and the Environment" in Environmental Conflict, p. 175

The first and most obvious conclusion is that there is no uniform relationship between democracy and the environment. Three of our indicators, deforestation, C02 emissions, and soil erosion by water, demonstrated significant negative relationships between democracy and environmental preservation. Protected land area showed a positive relationship, and freshwater availability and soil erosion by chemicals demonstrated no significant relationship. Of even greater interest, perhaps, is the fact that these relationships ran counter to expectation (Gleditsch and Sverdrup, 1996; Payne, 1995a). Instead of positive relationships between the extent of democracy and environmental protection, as much popular and recent scholarly writings have suggested, the associations found here are principally negative or nonexistent. This should give pause to political leaders such as President Clinton and Vice President Gore who have trumpeted the virtues of democracy in protecting the environment.

### 2AC---Disease

#### Considering Covid started in China, view this with a high amount of skepticism. Also they haven’t read an impact.

Kavanagh '20 - directs Georgetown University's Global Health Policy & Politics Initiative at the O'Neill Institute for National and Global Health [Matthew, "Authoritarianism, outbreaks, and information politics," The Lanet, VOLUME 5, ISSUE 3, E135-E136, MARCH 01, 2020]

For Amartya Sen, authoritarian states face serious challenges in information and accountability.6 Governments in closed political systems, without open media and opposition parties, struggle to receive accurate information in a timely manner and to convey urgent information to the public. Governments can be the victims of their own propaganda, because the country's political institutions provide incentives to local officials to avoid sharing bad news with their central bosses and await instructions before acting.

Information politics in China undermined a rapid response to the 2019-nCoV outbreak. Health-care workers suspected an outbreak in early December, 2019,7 but information with which the public might have taken preventive measures was suppressed, and communication channels that might have alerted senior officials to the growing threat were shut down.8 Police detained a clinician and seven other people posting reports on 2019-nCoV, threatening punishment for spreading so-called rumors. Social media was censored; a preliminary analysis of Weibo and WeChat published on China's biggest online platform9 showed outbreak discussions were nearly non-existent through much of January, 2020, until the Chinese Government changed its official stance on Jan 20, 2020.

Through much of January, 2020, the Wuhan Municipal Health Commission reported no evidence of human-to-human transmission, no infection among health workers, that severe cases of disease caused by 2019-nCoV infection were confined to those with underlying conditions and older people, and that the Huanan seafood market was the source.11 Reports in The Lancet7 and New England Journal of Medicine,12 however, show that half of patients admitted to intensive-care units were aged 25–49 years, and two-thirds had no underlying illnesses. Human-to-human transmission and health-worker infection were evident before the Chinese Government made an announcement.12 This information either did not make it to authorities or the public were misinformed. The Mayor of Wuhan has said publicly that not only was information not revealed in a timely manner but also they did not use information effectively.10 By the time quarantine went into effect on Jan 23, 2020, five million people had left the city of Wuhan for holiday travel.10 Outbreaks were subsequently reported throughout China.

Without open media and an opposition to check on bureaucratic hierarchy, knowledge from the front lines of the 2019-nCoV outbreak did not reach Beijing. Weeks into the outbreak, leaders were forced to publicly threaten that officials withholding information “will be nailed on the pillar of shame for eternity”.4

Is there an authoritarian advantage in disease response? It seems that authoritarian information politics inhibited a rapid response to the 2019-nCoV outbreak in China, which could have limited the crisis. It is not yet clear if the extraordinary cordons and influx of resources enabled by autocratic rule will prove a successful public health strategy. Yet, in building capacity to prevent, detect, and respond to outbreaks, democratic openness and competitive politics seem more asset than inadequacy.

### 2AC---Extinction !---Democracy

#### Democracy solves extinction

Kaushik Basu 21, former chief economist of the World Bank and chief economic adviser to the government of India, professor of economics at Cornell University and a nonresident senior fellow at the Brookings Institution. 12/24/21. <https://www.japantimes.co.jp/opinion/2021/12/24/commentary/world-commentary/protecting-democracy/> //pipk

NEW YORK – U.S. President Joe Biden’s recent Summit for Democracy was an important global event, but it slipped by almost unnoticed.

With democratic norms fraying from Southeast Asia to Central Europe, Biden was right to warn of “the sustained and alarming challenges to democracy and universal human rights.” But too few acknowledge that rising authoritarianism around the world, like climate change and the evolution of lethal viruses, can pose an existential risk to humanity.

Most people do not appreciate the extent to which civilizations depend on pillars of norms and conventions. Some of these have evolved organically over time, while others required deliberation and collective action. If one of the pillars buckles, a civilization could well collapse.

Efforts to counter the current threats to democracy should start with the fact that every economy is embedded in culture and institutions. As Daron Acemoglu, Simon Johnson, and James Robinson have argued, long-run growth may depend more on institutions than on anything else. But institutions are not always exogenous. As the growing field of cultural evolution shows, human beings are adaptive learners who rely, often unwittingly, on social learning to entrench norms that are necessary for a society to flourish.

Likewise, Avinash Dixit and Simon Levin argue that, in some contexts, we may need to take deliberate steps to instill pro-social preferences that can help us adapt to our changing world. We can do this through education, and by deliberating and deciding as citizens to promote certain kinds of collective behavior. That is what happened when delegates from American states convened in Philadelphia in 1787 to revise the existing Articles of Confederation and ended up drafting the U.S. Constitution, which became the cornerstone of the new country’s long-term growth and prosperity.

We are in a similarly challenging situation today, as cross-border flows of goods, services, and capital flatten the world economically. The rapid advance of digital technology, accelerated over the last two years by the COVID-19 pandemic, is causing huge strains. Increased outsourcing of production has contributed to hypernationalism, which in turn is fueling the rise of anti-democratic leaders who exploit people’s desperation.

These changes have come so swiftly that deliberate collective action is needed to defend democracy. We do not have the luxury of waiting for our norms and institutions to evolve.

### 2AC---Warming !---Democracy

#### Democracy solves climate change

Daniel J. Fiorino 19, Director of the Center for Environmental Policy at American University in Washington DC. Former Associate Director of the Office of Policy Analysis, EPA. "Improving Democracy for the Future: Why Democracy Can Handle Climate Change" June 24. <https://www.e-ir.info/2019/06/24/improving-democracy-for-the-future-why-democracy-can-handle-climate-change/> //pipk

The world seems to be following a pattern in which the more we learn about the rate and effects of climate change, the more there is to worry about. With every new scientific assessment, it appears that sea levels are rising more than anticipated, more species are being lost, glaciers are melting at surprising rates, droughts and floods are more severe, and extreme weather is on the rise. The Intergovernmental Panel on Climate Change (IPCC) warned that limiting average global temperatures to 1.5°C, as governments agreed to aim for in the 2015 Paris Climate Agreement, “would require rapid, far-reaching and unprecedented changes in all aspects of society” (IPCC 2018). The expert consensus in these reports is that emissions must fall dramatically by 2030 and the world should achieve a version of carbon neutrality by 2050.

The existential magnitude of the effects of a changing climate and modest progress in dealing with the causes (largely related to energy, transportation, agriculture, and forestry) so far leads critics to call for dramatic changes in governance. James Lovelock, prominent scientist and founder of the Gaia theory, argues, “Even the best democracies agree that when a major war approaches, democracy must be put on hold for the time being. I have a feeling that climate change may be an issue as severe as a war. It may be necessary to put democracy on hold for a while” (Hickman 2010). Other critics go even further, arguing that “humanity will have to trade its liberty to live as it wishes in favor of a system where survival is paramount” (Shearman and Smith 2007). Even restrained critics have concluded “it is not entirely clear that democracy is up to the challenge of climate change” (Jamieson 2014, 100).

Is democracy a barrier to acting on the causes and eventually the consequences of climate change? Is it time to toss the practical and normative benefits of democratic institutions, rights, and processes to meet an existential challenge? Is there any merit to the case against democracy? These are the issues I consider in my recent book, Can Democracy Handle Climate Change (Polity 2018).

The Cases for and against Democracy

The case made by critics of democracy goes something like this: Democracies exist to serve the needs and preferences of their citizens. They are built on notions of individual freedom and private property rights. Voters lack the needed scientific literacy to be able to understand the causes and consequences of climate change, and they are too focused on enjoying and expanding their affluence. Handling climate change calls for drastic action, perhaps a suspension of individual rights, hard controls on population and economic growth, and more modest lifestyles.

Given these flaws, critics argue that what is needed is top-down, centralized, and authoritarian governance by scientific (or at least scientifically enlightened) elites. With the appropriate concentrations of authority and ability to set aside constraints like private property rights and economic freedoms, enlightened autocrats can make hard choices and overcome vested interests. Only more authoritarian systems can take long view and force needed changes in societies and economics, a view that goes back to the early days of the modern environmental movement (e.g. Ophuls 1977).

There are many problems with this conception. The first is that no such benign ecological autocracy has ever existed. Although many critics hold out hope that an authoritarian China will lead the way, there are many reasons to doubt that scenario. Another is that the research does not support the view that democracies are less suited to handling climate change than authoritarian regimes. Although democracies appear to be better at devising policies than actually carrying them out, there is no evidence that they are inherently less capable of handling climate change than their authoritarian counterparts. Indeed, the reverse is more likely. It also is hard to imagine how these enlightened ecological autocrats will establish legitimacy and be able to make and carry out the tough decisions that have to be made. Why should we assume that political systems that cannot agree on a carbon tax will magically transform themselves into climate-action-above-all regimes?

Finally, the emergence of authoritarian populism in countries like Hungary, Poland, Venezuela, and even the United States do not bode well for a climate action agenda (Schaller and Carius 2019). As the quality of democracy and governance decline, so will capacities for dealing with climate change. Climate policy has suffered in regimes that reject scientific evidence, focus narrowly on the short term, assert extreme nationalism, and ally themselves strongly with established economic interests. If brief, the central flaw with visions climate-friendly autocracy that that no such system has ever existed. With liberal democracy breaking down in many places, these barriers to action will only increase. The quality as well as existence of democracy will matter for tackling climate change.

Comparing Democratic and Authoritarian Systems

Climate change is a complex challenge, the largest collective action problem in history, and a classic illustration of the concept of a wicked problem. It is distinctive in many ways: unlike most forms of air or water pollution, the effects are not immediately obvious; harms occur mostly in the future, with a perceived temporal mismatch of costs and benefits. Scientific uncertainty allows opponents of action at least to raise doubt. Further, acting on the causes of the problem require basic changes in economic and social systems, not just incremental fine-tuning.

There is good reason to believe, however, that democracies overall are more suited to handling climate change than their authoritarian counterparts. Among the reasons studied in the literature are the relatively free flows of information on problems and solutions in democracies; their administrative capacities and lower levels of corruption; their more active engagement in global problem-solving; multiple points of access in policy making (pluralism); superior scientific and technical capacity; and dynamic, innovative economies. Overall better governance capacities, such as less corruption, are part of their advantage (Dasgupta and De Cian 2018; Povitkina 2018).

The research on the climate capacities of democracies (almost all on mitigation) strongly suggests they are no less and probably more capable then authoritarian regimes (Fiorino 2018a). A 2013 study of national policies found that a history of and experience with democracy mattered; countries with “accumulated stock of civic and social assets built by experience with democracy” generally have better climate mitigation laws and policies (Fredriksson and Neumayer 2013, 11). In another study of climate policy, authoritarian regimes did not perform better than established democracies: “countries representing the capitalistic autocratic model like Russia, China, and in some measure Singapore lag far behind the democracies” (Kneuer 2012, 871).

#### Trump doesn’t disprove---US democracy still allowed a role for the states, improving solves federal action

Daniel J. Fiorino 19, Director of the Center for Environmental Policy at American University in Washington DC. Former Associate Director of the Office of Policy Analysis, EPA. "Improving Democracy for the Future: Why Democracy Can Handle Climate Change" June 24. <https://www.e-ir.info/2019/06/24/improving-democracy-for-the-future-why-democracy-can-handle-climate-change/>

Democracy critics often point to recent experience in the United States, where the Trump administration has reversed nearly every climate initiative of the Obama administration and announced its intent to withdraw from the 2015 Paris agreement. Here is a long-standing, highly consolidated democracy moving, at least nationally, in an entirely wrong direction. To be sure, these policy reversals do not bode well for democratic arguments about climate change. Yet the United States also illustrates the strengths of democracies: pluralism, innovation, open flows of information, and political accountability. In particular, federalism enables states—California, New York, Washington, and Hawaii, among them—to act as innovative clean energy and climate leaders (Roberts 2019).

Why the Democracy Issue Matters

Lovelock has said that surviving climate change “may require, as in a war, the suspension of democratic government for the duration of the survival emergency” (2009, 95). The problem is that this will be a perpetual war. Climate change is not something one just solves. Mitigating its causes and adapting to its effects is a constant struggle. And democracy is not something we can put on the shelf and revive when a crisis passes, if it does. Politics does not work in that way. The heart of sustainability is that the current generation should not close off options for future generations. A manageable climate is only part of what is left to future generations. Also handed down are systems of governance and such values as dignity, equity, and rights (Beckman 2008).

In practical terms, calls for a transition to an ecological authoritarianism imply three goals. One is to convert existing democracies into something very different for the duration of the climate emergency. The second is to abandon support for emerging democracies. The third is to anoint existing authoritarians as climate leaders and expand their influence in global action. The first is a high-risk strategy that sacrifices the practical and normative benefits of democracy for unknown and unpredictable alternatives. The second will undermine democratic transitions in countries whose political development will better equip them for effective action. The third legitimizes the very regimes whose commitment to climate mitigation is highly uncertain. All of these involve risks not only to the climate but to global stability and sustainable development.

Of course, we can hope that authoritarian as well as democratic political systems make the transition to zero-carbon, climate-friendly economies and societies. Indeed, it is essential; authoritarian and hybrid systems in the Economist Intelligence Unit’s Democracy Index account for about one-half of global greenhouse gas emissions (Fiorino 2018a, 22). But to argue they are inherently superior or we should transform political systems to pursue an idealized ecological autocracy is dangerous, not only for the climate but for human well-being more generally.

The path lies not in suspending democracy but improving it: create better democracies with the capacity for collective action and a commitment to ecological values. The most effective strategy lies in fostering the political, social, and economic conditions in which democracies will flourish, not only for the sake of the planet but for the dignity and welfare of future generations.

### 2AC---Authoritarianism !---Democracy

#### Democracy prevents authoritarianism---outweighs and causes extinction

Tom Barnes & Marie Davidsen Buhl 21. Visiting Fellow & Research Intern at Rethink Priorities. PhD student in the Environmental Systems (ES) program at the University of California, Merced. <https://rethinkpriorities.org/publications/towards-a-longtermist-framework-for-evaluating-democracy-related-interventions> //pipk

Preventing the risk of societies coming under the control of a single group/leader, who hold exclusive political power. At its extreme, this could include totalitarianism. Taking preventative measures to stop democratic backsliding may help to prevent authoritarianism.

What are some ways authoritarianism might affect the long-term future?

Existential risk reduction: Malevolent actors (Althaus and Baumann, 2020) who become authoritarian leaders may potentially inflict astronomical levels of suffering, perhaps locking humanity into an undesired or enforced dystopia, and potentially leading humanity into a fate worse than mere extinction. An alternative existential risk may be that authoritarian leaders are less competent at dealing with other x-risks, such as the development of new technology. Thus authoritarianism may increase existential risk indirectly. A further worry is that humanity may never achieve its full potential - for instance, a stable authoritarian leader could prevent space colonization from occurring, leaving vast amounts of the galaxy without value. This would also constitute an existential risk via a failed continuation.

Trajectory change: A less extreme worry may be that authoritarian leaders fail to address certain sources of disvalue, even if humanity still enjoys a flourishing future. For example, they may not prevent wild animal suffering on Earth even if most of the universe is filled with value.

What are some ways democracy might affect authoritarianism?

Competitive democracy: Efforts to improve competitive democracy make it easier to remove leaders from power in elections, which can reduce the risk of authoritarianism arising.

Responsiveness & accuracy: The extent to which increasing these features makes authoritarianism more or less likely depends on the preferences of voters. For example, if voters tend to prefer non-authoritarian leaders, then increasing how well the political system responds and reflects voters’ preferences makes authoritarianism less likely. Conversely, if voters prefer more authoritarian leaders, then adjusting the political system to accommodate for this makes higher responsiveness/accuracy more likely to bring about authoritarianism. It seems likely that, on average, most democratic citizens would prefer less rather than more authoritarianism in their political system (however, this is very context-dependent).

Participation: Countries with high levels of participation seem more likely and better able to challenge an authoritarian leader, compared to where apathy is high or participation is curtailed. Additionally, because authoritarian regimes may try to limit participation, means of keeping participation high once an authoritarian first gains power could be an especially important way to prevent authoritarianism from being locked in.

Liberalism: Authoritarianism and liberalism are almost polar opposites – societies high in liberalism are far less likely to see an authoritarian rise to power. For example, because liberalism safeguards pluralism, multiple value systems and beliefs are allowed to co-exist, whereas authoritarian regimes tend to exclude values that deviate from orthodoxy.

Voter competence: Democracies with low levels of well-informed voters may be more susceptible to polarisation and populism, which can in turn be a driver of electing authoritarian leaders. Thus, efforts to increase voter competence may reduce the likelihood of authoritarianism.

### 2AC---Turns Growth

#### Democracy key to growth---their ev uses bad models

Daron Acemoglu et al 19, Professor of Economics at MIT. Suresh Naidu Columbia University Pascual Restrepo Boston University James A. Robinson University of Chicago. Journal of Political Economy "Democracy Does Cause Growth" //pipk

We provide evidence that democracy has a positive effect on GDP per capita. Our dynamic panel strategy controls for country fixed effects and the rich dynamics of GDP, which otherwise confound the effect of democracy. To reduce measurement error, we introduce a new indicator of democracy that consolidates previous measures. Our baseline results show that democratizations increase GDP per capita by about 20 percent in the long run. We find similar effects using a propensity score reweighting strategy as well as an instrumental-variables strategy using regional waves of democratization. The effects are similar across different levels of development and appear to be driven by greater investments in capital, schooling, and health.

I. Introduction With the spectacular economic growth under nondemocracy in China, the eclipse of the Arab Spring, and the recent rise of populist politics in Europe and the United States, the view that democratic institutions are at best irrelevant and at worst a hindrance for economic growth has become increasingly popular in both academia and policy discourse. For example, the prominent New York Times columnist Tom Friedman (2009) argues that “one-party nondemocracy certainly has its drawbacks. But when it is led by a reasonably enlightened group of people, as China is today, it can also have great advantages. That one party can just impose the politically difficult but critically important policies needed to move a society forward in the 21st century.” Robert Barro (1997, 1) states this view even more boldly: “More political rights do not have an effect on growth.”

Although some recent contributions estimate a positive effect of democracy on growth, the pessimistic view of the economic implications of democracy is still widely shared. From their review of the academic literature until the mid-2000s, Gerring et al. (2005, 323) conclude that “the net effect of democracy on growth performance cross-nationally over the last five decades is negative or null.”

In this paper, we challenge this view. Using a panel of countries from 1960 to 2010, we estimate the impact on economic growth of the unprecedented spread of democracy around the world that took place in the past 50 years. The evidence suggests that democracy does cause growth and that its effect is significant and sizable.1 Our estimates imply that a country that transitions from nondemocracy to democracy achieves about 20 percent higher GDP per capita in the next 25 years than a country that remains a nondemocracy. The effect of democracy does not depend on the initial level of economic development, although we find some evidence that democracy is more conducive to growth in countries with greater levels of secondary education.

The estimation of the causal effect of democracy (or a democratization) on GDP faces several challenges. First, existing democracy indices are subject to considerable measurement error, leading to spurious changes in democracy scores that do not correspond to real changes in democratic institutions.

Second, democracies differ from nondemocracies in unobserved characteristics, such as institutional, historical, and cultural aspects, that also have an impact on their GDP. As a result, cross-country regressions, as those in Barro (1996, 1999), could be biased and are unlikely to reveal the causal effect of democracy on growth. Recent studies tackle this problem by using difference-in-differences or panel data estimates with country fixed effects.

Third, as shown in figure 1, as well as in Acemoglu et al. (2005) and Brückner and Ciccone (2011), democratizations are, on average, preceded by a temporary dip in GDP. This figure depicts GDP dynamics in countries that democratized at year 0 relative to other countries that remained nondemocratic at the time. The pattern in this figure implies that failure to properly model GDP dynamics, or the propensity to democratize based on past GDP, will lead to biased estimates of democracy on GDP. Though largely overlooked in previous work, the dip in GDP that precedes a democratization constitutes a clear violation of the paralleltrends assumption that underlies the difference-in-differences or panel data estimates used in the literature. Modeling GDP dynamics would also enable an investigation of whether the impact of democratization on GDP is short-lived or gradual.

Last but not least, even if we control for country fixed effects and GDP dynamics, changes in democracy could be driven by time-varying unobservables related to future economic conditions, potentially leading to biased estimates.

In this paper, we address these challenges. We build on the important work by Papaioannou and Siourounis (2008) to develop a dichotomous measure of democracy, which combines several indices to purge spurious changes in each. We rely on this measure for most of our analysis but also document the robustness of our results to other measures of democracy in the online appendix.

There is no perfect strategy for tackling the remaining challenges and estimating the causal effect of democracy on GDP. Our approach is to use a number of different strategies, which reassuringly all give similar results. Our first approach uses a dynamic (linear) panel model for GDP, which includes both country fixed effects and autoregressive dynamics. The underlying economic assumption here is that, conditional on the lags of GDP and country fixed effects, countries that change their democratic status are not on a differential GDP trend (and thus these lags successfully model the dip in GDP that precedes democratizations shown in fig. 1). This strategy leads to robust and precise estimates that indicate that in the 25 years following a permanent democratization, GDP per capita is about 20 percent higher than it would be otherwise.

Our second strategy adopts a semiparametric treatment effects framework in which democratization—the treatment—influences the distribution of potential GDP in all subsequent years. This strategy requires us to model the process of selection into democracy as a function of observables, in particular, lags of GDP (e.g., Jordà 2005; Angrist and Kuersteiner 2011; Kline 2011), but it does not rely on a parametric model for the dynamics of GDP, which affords us greater flexibility in estimating the time path of the impact of democracy on GDP. Related to our first approach, the economic assumption in this case is that, conditional on the lags of GDP, countries that democratize are not on a differential GDP trend relative to other nondemocracies. We show that this approach successfully controls for the influence of the dip in GDP preceding democratizations shown in figure 1 and estimates that after a democratization, GDP increases gradually until it reaches a level 20–25 percent higher than what it would reach otherwise.

These two strategies model the selection of countries into different regimes and control for the dip in GDP in figure 1 as a function of their re cent GDP per capita and time-invariant unobserved heterogeneity. However, they do not tackle the possibility that both democracy and GDP might be affected by time-varying omitted variables. Our third strategy confronts this challenge by using an instrumental-variables (IV) approach. The political science literature emphasizes that transitions to democracy often take place in regional waves (e.g., Huntington 1991; Markoff 1996). On the basis of this observation, we use regional waves in transitions to and away from democracy as an instrument for country-level democracy. Our IV strategy exploits the diffusion of political regimes across countries in the same region and with common political histories. We pay special attention to distinguishing the diffusion of democracy from the role of regional economic shocks or the spread of economic conditions to nearby countries through trade and other mechanisms. By focusing on the variation created by regional waves of democratizations, our IV strategy ensures that idiosyncratic changes in a country’s political regime that may be endogenous to its growth do not bias our estimates. The resulting estimates of the impact of democracy on GDP are similar to those from our other two strategies: in our preferred specification, a democratization increases GDP per capita by about 25 percent in the first 25 years—although in some specifications the estimated effects are larger. This similarity bolsters our confidence that all three of our strategies are estimating the causal effect of democracy on GDP.

We further investigate the channels through which democracy increases GDP. Although our findings here are less clear-cut than our baseline results, they suggest that democracy contributes to growth by increasing investment, encouraging economic reforms, improving the provision of schooling and health care, and reducing social unrest. These results are consistent with, though of course do not prove, the hypothesis that democracies invest more in broad-based public goods and are more likely to enact economic reforms that would otherwise be resisted by politically powerful actors (e.g., Acemoglu 2008). Although nondemocracies could also invest in public goods or enact far-ranging economic reforms, our results indicate that, at least in our sample, these countries are less likely to do so than democracies.

At the end of the paper, we turn to the common claim that democracy constrains economic growth for countries with low levels of development (e.g., Aghion, Alesina, and Trebbi 2008; Posner 2010; Brooks 2013). Our results do not support this view, but we do find that democracy has a larger impact on growth in countries where a greater fraction of the population has secondary schooling.

There is a substantial literature in political science that investigates, but does not reach a firm conclusion on, the empirical linkages between democracy and economic outcomes, summarized in part in Przeworski and Limongi (1993) and in Doucouliagos and Ulubaşoğlu’s (2008) meta-analysis.

Cross-country regression analyses, such as Helliwell (1994), Barro (1996, 1999), and Tavares and Wacziarg (2001), have produced negative, though generally inconsistent, results.2 More recent work, including Rodrik and Wacziarg (2005), Persson and Tabellini (2006), Papaioannou and Siourounis (2008), and Bates, Fayad, and Hoeffler (2012), estimate positive effects using panel data techniques, although Murtin and Wacziarg (2014), Burkhart and Lewis-Beck (1994), and Giavazzi and Tabellini (2005) estimate insignificant effects on growth using similar strategies.3 These and other papers in this literature differ in their measure of democracy and choice of specifications and neither systematically control for the dynamics of GDP nor address the endogeneity of democratizations. Although some of the papers in this literature control for lags of GDP in some of their specifications (e.g., Persson and Tabellini 2006; Papaioannou and Siourounis 2008; Murtin and Wacziarg 2014), they do not emphasize the importance of GDP dynamics and the bias that results from not appropriately controlling for the dip in GDP shown in figure 1. The failure to recognize this point may, in fact, explain the divergent results in the literature: because growth rates are less serially correlated than GDP, contributions that focus on growth as the dependent variable tend to find positive effects, while studies that estimate models in levels generally find no effects—unless they model the dynamics of GDP as we do.

### 2AC---Turns Innovation

#### Democracies key to innovation

Tom Barnes & Marie Davidsen Buhl 21. Visiting Fellow & Research Intern at Rethink Priorities. PhD student in the Environmental Systems (ES) program at the University of California, Merced. <https://rethinkpriorities.org/publications/towards-a-longtermist-framework-for-evaluating-democracy-related-interventions> //pipk

What is this potential intermediate goal?

For our purposes, intellectual progress includes (but isn’t limited to) technological advancement, scientific progress, progress in philosophy and the social sciences, and increases in general levels of education and reasoning ability. “Progress” is meant as a value-neutral term; some advancements could do more harm than good.

What are some ways intellectual progress might affect the long-term future?

Speeding up development: If new discoveries in science, technology and ideas are made quicker, it allows humanity to reach a better state faster than it otherwise would.

Existential risk (and trajectory changes): There is a need for differential progress, whereby intellectual progress in risk-reducing factors (e.g., wisdom) ought to come before risk-increasing factors (e.g., knowledge of bioweapon construction). Otherwise, faster intellectual progress could increase existential risk.

Meta-longtermism: A better educated population focused on doing impactful/useful work will be more capable of making progress on other longtermist areas.

Crucially, intellectual progress may either increase or decrease existential risk, depending on the particular form of progress being made. Thus, it is difficult to determine whether such progress is all-things-considered good or bad. Further research is required to delineate specifically which forms of progress are good or bad for the long term.

What are some ways democracy might affect intellectual progress?

Participation: Anti-democratic regimes may see new ideas as a threat to their authority, which would incentivise them to restrict the discovery and proliferation of new ideas. To do this, they may seek to exclude or eliminate intellectuals[11]. Additionally, some countries may make it harder for educated/intellectual groups to participate in decision making (e.g., by shrinking the influence of academics on policy). Thus, democracies low in participation could create less intellectual progress.

### 2AC---AT: Democracy Bad

#### Democracy solves every impact---it’s comparatively more stable than autocracies

Matt Kroenig 20, Professor of government and foreign service at Georgetown. 4/3 “Why the U.S. Will Outcompete China” <https://www.theatlantic.com/ideas/archive/2020/04/why-china-ill-equipped-great-power-rivalry/609364/>

National-security analysts see China as one of the greatest threats facing the United States and its allies. According to an emerging conventional wisdom, China has the leg up on the U.S. in part because its authoritarian government can strategically plan for the long term, unencumbered by competing branches of government, regular elections, and public opinion. Yet this faith in autocratic ascendance and democratic decline is contrary to historical fact. China may be able to put forth big, bold plans—the kinds of projects that analysts think of as long term—but the visionary projects of autocrats don’t usually pan out. Watch White Noise, the inside story of the alt-right The Atlantic’s first feature documentary ventures into the underbelly of the far-right movement to explore the seductive power of extremism. Stream Now Yes, democratic governments are obligated to answer to their citizens on regular intervals and are sensitive to public opinion—that’s actually democracies’ greatest source of strength. Democratic leaders have a harder time advancing big, bold agendas, but the upside of that difficulty is that the plans that do make it through the system have been carefully considered and enjoy domestic support. Historically speaking, once a democracy comes up with a successful strategy, it sticks with the plan, even through a succession of leadership. Washington has arguably followed the same basic, three-step geopolitical plan since 1945. First, the United States built the current, rules-based international system by providing security in important geopolitical regions, constructing international institutions, and promoting free markets and democratic politics within its sphere of influence. Second, it welcomed into the club any country that played by the rules, even former adversaries, like Germany and Japan. And, third, the U.S. worked with its allies to defend the system from those countries or groups that would challenge it, including competitors such as Russia and China, rogue states such as Iran and North Korea, and terrorist networks. America can pursue long-term strategy in part because it enjoys domestic political stability. While new politicians seek to improve on their predecessor’s policies, the United States is unlikely to see the drastic shifts in strategy that come from the fall of one political system and the rise of another. Democratic elections may be messy, but they’re not as messy as coups or civil wars. Daniel Blumenthal: The Unpredictable Rise of China Open societies have many other advantages as well. They facilitate innovation, trust in financial markets, and economic growth. Because democracies tend to be more reliable partners, they are typically skillful alliance builders, and they can accumulate resources without frightening their neighbors. They tend to make thoughtful, informed decisions on matters of war and peace, and to focus their security forces on external enemies, not their own populations. Autocratic systems simply cannot match this impressive array of economic, diplomatic, and military attributes. David Leonhardt recently wrote in The New York Times, “Chinese leaders stretching back to Deng Xiaoping have often thought in terms of decades.” Commonly cited examples of that long-term thinking include the Belt and Road Initiative, a program that invests in infrastructure overseas; Made in China 2025, an effort to subsidize China’s giant tech companies to become world leaders in 21st-century technologies, such as artificial intelligence; and Beijing’s promise to be a global superpower by 2049. Since putting in place sound economic reforms in the 1970s, China has seen its economy expand at eye-popping rates, to become the world’s second largest. Many economists predict that China could even surpass the United States within the decade, and some have suggested that China’s model of state-led capitalism will prove more successful, in terms of economic growth, than the U.S. template of free markets and open politics. I doubt these predictions. Because autocratic leaders are unconstrained and do not have to contend with a legislature or courts, they have an easier time taking their countries in new and radically different directions. Then, when the dictator changes his mind, he can do it again. Mao’s autocratic China ricocheted from one failed policy to another: the Great Leap Forward, then the Hundred Flowers Campaign, then the Cultural Revolution. Mao aligned with the Soviet Union in 1950 only to nearly fight a nuclear war with Moscow in the next decade. Beginning in the time of Deng Xiaoping, China pursued a fairly constant strategy of liberalizing its economy at home and “hiding its capabilities and biding its time” abroad. But President Xi Jinping abandoned these dictums when he took over. As the most powerful leader since Mao—he has changed China’s constitution to set himself up as dictator for life—he could once again jerk China in several new directions, according to his whims, and back again. According to the Asia Society, he has stalled or reversed course on eight of 10 categories of economic reform promised by the Chinese Communist Party (CCP) itself. Moreover, Xi is baring China’s teeth militarily, taking contested territory from neighbors in the South China Sea and conducting military exercises with Russia in Europe. The problem for Beijing is that stalled reforms will stymie its economic potential and its confrontational policies are provoking an international coalition to contain them. The 2017 U.S. National Security Strategy declared great-power competition with China the foremost security threat to the U.S.; the European Union labeled China a “systemic rival”; and Japan, Australia, India, and the United States have formed a new “quad” of powers to balance China in the Pacific. Furthermore, the plans often cited as evidence of China’s farsighted vision, the Belt and Road Initiative and Made in China 2025, were announced by Xi only in 2013 and 2015, respectively. Both are way too recent to be celebrated as brilliant examples of successful, long-term strategic planning. A certain level of domestic political stability is a prerequisite for charting a steady strategic course in foreign and domestic affairs. But autocratic regimes are notoriously brittle. While institutionalized political successions in democracies typically lead to changes of policy, political successions in autocracies are likely to result in regime collapse and war. China’s “5,000 years of history” were pockmarked by rebellion, revolution, and new dynasties. Fearing internal threats to domestic political stability—consider the protests this year in Hong Kong and Xinjiang—the CCP spends more on domestic security than on its national defense. If you follow the money, the CCP is demonstrating that the government is more afraid of its own people than of the Pentagon. This domestic fragility will frustrate China’s efforts to design and execute farsighted plans. If threats to Chinese domestic stability were to materialize and the CCP were to collapse tomorrow, for example, Chinese grand strategy could undergo another seismic shift, including possibly opting out of competition with the United States altogether. Shadi Hamid: China Is Avoiding Blame by Trolling the World Autocracies have other vulnerabilities as well. State-led planning has never produced high rates of economic growth over the long term. Autocrats are poor alliance builders who fight with their supposed allies more than with their enemies. And the highest priority of autocratic security forces is repressing their own people, not defending the country. The world has undergone drastic changes in just the past few years, but these enduring patterns of international affairs have not. Some fear that Trump’s nationalist tendencies will erode the U.S. position, but the momentum of America’s successful grand strategy has kept the country on a fairly steady course. Despite Trump’s criticism of NATO, for example, two new countries have joined the alliance on his watch, including North Macedonia this week. The coronavirus has upended a sense of security in the U.S., leading many people into the familiar trap of lauding autocratic China’s firm response in contrast to the halting and patchwork measures in the United States. But there is good reason to believe that this assessment will be updated in America’s favor with the benefit of hindsight. Already we are seeing evidence that conditions are much worse in China than CCP officials are letting on and that China’s attempts at international “disaster diplomacy” are backfiring. It has been revealed that the CCP has continually misrepresented the numbers of COVID-19 infections and deaths in China, and European nations have rejected and returned faulty Chinese coronavirus testing kits.

## Solvency

### 2AC---Pilot Project Solvency---Logistics

#### Starting with logistics pilot projects spills over to effective NATO AI cooperation more broadly---it creates buy-in and prepares the Alliance technologically, socially, and politically

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

NATO and its Allies have strong reasons to adopt a pragmatic approach, which can be conveniently defined as 3S: small + secure = success. The rationale is as follows: • Small: small projects are unlikely to generate internal opposition or face major challenges; • Secure: secure projects are also at lower risks of technical or organizational failure; • Success: success is thus more readily within reach.

According to Google Brain’s co-founder Andrew Ng, for instance, it “is important for [the] first few AI project to succeed rather than be the most valuable AI projects”. This means they should be “technically feasible” and have “a clearly defined and measurable objective that creates business value”.134 Greg Allen, now at the US Department of Defense’s Joint Artificial Intelligence Center, reiterates this message from a different angle. He considers that many “AI projects fail not because of the technology, but because of a failure to properly set expectations, integrate with legacy systems, and train operational personnel”.135 Militaries have learned these lesson in previous instances of technological change: historically, many breakthrough technologies generated opposition, they did not deliver on their promises, and the increases in costs and time requirements further undermined their acceptance.136 As such, a pragmatic approach to small and feasible projects minimizes the chance that political or technical failure might slow down the Alliance’s adoption of AI.

A pragmatic approach to “NATO-mation” follows two key assumptions. First, many discussions about AI currently focus on the tension between narrow versus general AI. Some believe that the age of “the singularity” – where general AI will be superior to human intelligence – is near. Others believe that this is a remote dream and that, for the foreseeable future, intelligent machines will be able only to conduct limited, specific tasks.137 For the moment, the Alliance should just look at “narrow” AI. Second, the approach pursued by the Alliance should encompass a wide range of uses, and go beyond discussion limited to lethal autonomous weapons systems. The debate on lethal autonomous weapons systems that has taken place over the past few years has in fact distracted attention from the military relevance of AI and its broader implications for the international system. As David Judge, Vice President of SAP Leonardo, puts it, the conversation built around the question “Are we going to have red-eyed killer robots?” is not useful.138 Indeed, even insofar as the lethal debates are important, these are largely regulatory questions decided at the national level, rather than at NATO level. NATO would therefore be better advised to pursue the lines advanced by Judge: we “should instead focus on pragmatic uses of AI that are already here and ready”.139

While intellectual debates about these two assumptions are relevant to long-term patterns of adoption, current adoption efforts should focus on exploiting narrow AI below the tip of the spear. Such exploitation depends on investments in complementary assets, goods, services, and changes to business models. The San Francisco-based consultancy Altimeter contextualizes these investments in its four main phases of AI adoption: exploration, experimentation, formalization and integration, depicted in the diagram below.140

When it comes to defence and AI, most NATO Allies sit between exploration (phase 1) and experimentation (phase 2). Only a few have eyed formalization (phase 3), and even fewer have started looking at integration (phase 4). This last phase coincides with what in business is generally known as enterprise adoption: when a technology becomes pervasive in the work of an organization. It is important to highlight, however, that at this stage, in the commercial world, even the most AI-intensive, ML-savvy and data-hungry companies have hardly made it properly to phase 3.141 Microsoft, Google, Amazon, Baidu and Facebook can deploy advanced AI solutions because they have access to an unparalleled amount of data and top talent, and because they have invested billions and years in AI. Other actors that lack these resources and capabilities should initially be more focused.142

Security analysts and scholars are primarily concerned that first movers in the AI race could reap the benefits of this technological transformation, thus forcing others to a condition of technological dependence and military vulnerability. Business scholars advise caution, as the conditions for first mover’s and second mover’s advantage to take place are quite specific.143 What matters for this discussion is that NATO and its Allies neither have to rush into AI nor have the luxury to wait: they need to prepare, technologically but also socially and politically, in order to avoid potential backlashes or resistance. In order to pursue this goal, one strategy consists in adopting a pragmatic approach based on a set of small and secure pilot-projects that, as such, are more likely to achieve success. Three potential areas are:

Logistics. General Omar Bradley famously said that amateurs study tactics, professionals study logistics. Logistics is, in fact, a critical element of military operations – although often neglected among the public, and even among some experts.144 Logistic capabilities can in fact give significant combat advantages.145 This is a familiar story to NATO, whose forces have, at times, enjoyed massive logistic advantages vis-à-vis some of their adversaries.146 Logistics can be divided into layers: strategic, operational, in-theatre and on the battlefield. There is definitely room for employing AI at every level. Launching AI pilot projects in last-mile logistics (e.g., on the front line), however, has significant benefits. In particular, if Amazon or Domino Pizza aim to rely on automated drone-based delivery systems, there is no reason why NATO Allies cannot at least try a similar approach when it last-mile resupplies.147 The advantage of last-mile logistics is that, lying at the end of the tail, it does not entail major infrastructure investments. However, it is complex, difficult and often also dangerous. For this reason, even small improvements in this realm are going to have significant effects. NATO and its Allies could fund a project, or launch a DARPA-like Grand Challenge, to develop an autonomous system for last-mile logistics. DARPA’s Grand Challenges are open calls to the public at large for participating in a competition with a prototype. In Europe, the Joint European Disruptive Initiative has tried to replicate on a smaller scale DARPA’s model, with remarkable success so far.

#### Logistics pilot project solves---demonstrates value of AI and leads to effective cooperation---that’s key to international AI cooperation and ethical development

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

The increasing power of processors, accuracy of algorithms, and availability of digital data are driving the dramatic artificial intelligence (AI)-centred technological transformation now in progress. These changes have already turned companies, industries and markets upside down, and we are also starting to see their effects on the battlefield. The employment of unmanned vehicles, reliance on big data for target detection, identification and acquisition, as well as the potentials of machine learning in other critical functions such as logistics and maintenance are only some of the possible examples of how warfare will evolve in the near future. The North Atlantic Treaty Organization (NATO) and its Allies cannot be bystanders during this technological transition. Some countries and organizations have already taken important steps. Others are more hesitant. The Atlantic Alliance has a moral obligation to act, both to preserve and extend its military leadership – and thus the wealth and security of its citizens – and to shape this process in keeping with its democratic principles, freedom-inspired values and commitment to fundamental human rights. As NATO works on its Artificial Intelligence Strategy, which could be published in 2021, this Research Paper aims at contributing to both the policy debate and the public discussion about AI and its implications for the Alliance. The paper offers a series of analyses, lessons learned, proposals, and recommendations, that build on best practices and solutions adopted in the civilian and military fields, on perspectives drawn from the academic literature as well as on ideas generated in the broader AI community. The various parts of the paper are all linked to the single overarching concept of “NATO-mation”, or the idea that NATO has an important role to play so as to prepare for and to shape this technological transformation. NATO Allies need to be proactive: without common, coordinated, cooperative or joint solutions, they will not be able to achieve all their goals effectively and efficiently. The paper thus elaborates on the concept of “NATO-mation” in 11 different building blocks, as summarized below:

Ethical purpose: first and foremost, NATO’s strength comes from its values, which give meaning to its military capabilities and represent the bond between the Allies. As technological progress demands answers to major ethical questions regarding the development, employment and purpose of intelligent machines, NATO and its Allies have the opportunity to shape international norms and behaviour in this respect while simultaneously strengthening their commitment to the Alliance’s founding principles. Setting up an ethical board of experts and adopting some common ethical principles are two starting points.

Championing innovation: innovation is more difficult than generally accepted, often because of cognitive resistance, bureaucratic inertia or lack of political appetite. An important step forward would be to identify a champion within the Alliance, with a view to promoting, supporting and enabling the adoption of AI. This champion would work with Allies to connect and coordinate their activities and initiatives, as well as support them in key areas such as training or reform: a new structure could also be created, and could be called potentially an Artificial Intelligence Integration and Implementation-Enabling Centre (A3IC).

Pilot projects: innovation is often difficult because individuals and organizations are inherently risk-averse. NATO and its Allies should work on the 3S principle to address this aspect: start from small (S) and secure (S) pilot projects which can, through their success (S), readily and simply demonstrate the potential of these new technologies. Last-mile logistics, military medicine and disinformation are three areas where NATO could start working.

### 2AC---Pilot Project Solvency---NATO Key

#### AI effectiveness key to NATO---pilot projects solve enterprise-level adoption necessary for integration and leadership

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

According to many observers, artificial intelligence (AI), machine learning (ML) and big data (BD) are going to promote a dramatic technological transformation affecting every aspect of our lives, every industry and profession, every layer of our societies, with major implications also for international politics.5 The consequences for military affairs and international security are still not fully appreciated or understood.6 Nonetheless, building on previous cases, as well as historical experience with other major technological revolutions, we can reasonably conjecture that the fallout will likely be massive. Countries – and alliances – unable to adapt quickly and thoroughly will be left by the wayside.7 Understanding, preparing for and exploiting this technological transition is thus of utmost importance for NATO and for its Allies.8

The Atlantic Alliance as a whole has an obligation to preserve and extend its military power, maintain its level of prosperity and internal cohesion, lay the conditions for future wealth creation, and make its action more efficient and effective, starting from its core tasks: collective defence, crisis management and cooperative security.9 The technological transformation triggered by AI, ML and BD will, however, challenge many of the assumptions, procedures, capabilities, skills as well as doctrines and strategies underpinning NATO’s current activities.10 There can be no substitute for understanding, preparing and exploiting this AI-centred technological transition, but it will require significant effort.11 The first Industrial Revolution – driven by the combined employment of new mechanical devices – was ultimately about increasing the power of natural energy, and it brought about a dramatically different international system.12 Similarly, the second Industrial Revolution, which allowed for large production runs and thus brought economies of scale centre stage, made “mass” a central tenet of military power, with tragic consequences for international politics due to the emergence of industrial and total war.13 The third Industrial Revolution, with its focus on computation, allowed for much higher levels of precision; and precision came to dominate the battlefield – through long-range guided munitions, real-time intelligence, surveillance and reconnaissance assets and stealth, among others.14 Some define our new era as the fourth Industrial Revolution.15 Others speak of the Second Machine Age.16 Regardless of the name, in the age of intelligent machines, machine speed will likely prove one of the defining features of future warfare.17

NATO should act so that it can be at the forefront of this transition, rather than observe it as an onlooker or – even worse – be subjected to it by others. In order to avoid the risk of lagging behind, AI will have to be integrated across the board – i.e., in every single aspect and domain, layer and functional area: from data gathering and processing to communications and cyber-defence, from logistics and medical diagnosis to tactical, operational and strategic decision-making.18 Such enterprise-level adoption would allow Allied forces to run every single procedure and process at machine speed, and thus not find themselves outcompeted. Admittedly, enterprise adoption is challenging – even more so for AI, given that it requires different organizational solutions and culture, talent and skills, and infrastructure support.19

The defence and military capabilities of NATO countries are tightly integrated and coordinated, resulting in combined military power where the sum is greater than its parts. NATO and its Allies will have to integrate AI at enterprise level – in order to preserve their military and technological leadership in the near future – both at the national and coalition level.20 The challenge will thus be massive.

Building on existing academic research and policy discussions, including those related to a NATO Artificial Intelligence Strategy, 21 this Research Paper has a twofold purpose: to contribute to existing debate within the Alliance on AI, ML and BD, and key related issues; and to advance a number of proposals centred on the concept of “NATO-mation” – i.e., equipping the Alliance with the capabilities, organizational structures and strategies to compete in the world of AI.22

Given the major changes now under way, the Atlantic Alliance has a unique opportunity to shape this transformation, rather than sit by as an onlooker. With the concept of “NATO-mation”, this Research Paper aims to promote this goal. The research is based on two guiding principles. On the one hand, individual measures will be crucial to sustain and expand the Alliance’s economic, technological and hence military power, and adapt it to new circumstances and needs. On the other hand, coordination and cooperation among the Allies will be necessary to address the resulting challenges and ensure continued integration in the NATO context.23 Uncoordinated individual actions risk creating a major offset in capabilities among Allies, with a number of negative implications for interoperability, cohesion and consensus. Moreover, because of the very nature of the technologies at hand, the consequences of failure to work in concert could prove even more dramatic.24 The challenge is therefore not limited to technology per se, but includes other equally relevant domains. This is why discussion of the “NATO-mation” concept is divided into the following 11 building blocks: • Ethical purpose: making sure that NATO acts in the ethical domain, following and promoting its founding principles and moral commitments; • Championing innovation: identifying an innovation champion to lead, support, connect and engage with all Allies and relevant stakeholders; • Pilot projects: favouring adoption by promoting small, secure projects with greater likelihood of success; • An innovative workforce: understanding and addressing the human capital requirements this new transition entails; • An innovative workplace: changing organizations to attract and retain talent and thus enable innovation; • Concepts: running simulations, exercises and wargames to test and devise new concepts and technologies; • Technological superiority: maintaining and extending technological leadership and developing new relevant technologies; • Arms control and technology regimes: supporting mechanisms to strengthen international stability and prevent diffusion of critical technologies; • The data pipeline and the AI Network Trinity: promoting the development of the ecosystem necessary to exploit AI, including cloud and quantum computing and 5G networks; • Standards and standardization: enabling interoperability and translating strategic imperatives and ethical commitments into technological solutions; • Primacy of democracy: protecting democracy and democratic values against digital authoritarianism. For each of these building blocks, the paper will discuss the importance of the issue, the key challenges, potential solutions and possible recommendations.

### 2AC---Now Key

#### First mover advantage key to great power competition---failure to act now creates path dependencies that are impossible to overcome

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

For any country, and in particular for Great Powers, being at the forefront of science and technology is a priority, as it represents a key asset for both national security and prosperity. This is even more acute in an age of accelerating technological change. Many modern sectors of the economy as well as the defence realm require an advanced industrial, scientific and technological base that is extremely demanding to create.224 For countries that do not keep up with progress and are forced to exit some sectors, re-entry tends to be very difficult because of the need to recruit qualified people, acquire material capabilities, and – most daunting of all – develop the necessary organizational and technical experience.225 In other words, lagging behind today can create path dependencies that will then be extremely difficult to overcome in the future.226 This is particularly the case for AI, ML and BD, given that distinctive features such as decreasing marginal costs tending to zero, increasing return of scales and demand-side economies of scale (network externalities) make it difficult, if not impossible, to make up lost ground. Hence, for NATO countries it is of utmost importance to take proactive measures to avoid such a risk.227

### 2AC---Data-Sharing

#### Aff solves data-sharing

Erik Lin-Greenberg 20, postdoctoral fellow at the University of Pennsylvania’s Perry World House. Texas National Security Review, Vol 3, Iss 2. Spring. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making" <https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/> //pipk

Although the proliferation of military AI technology has the potential to frustrate alliance military operations and decision-making, these obstacles are not insurmountable. Allies have previously worked together on missions that involved new technology, shared highly sensitive information, and learned to cope with compressed decision-making timelines. Drawing lessons from historical exemplar cases where allies have wrestled with new technology, coupled with guidance from emerging national AI policies and analysis of new technologies, I identify ways that alliances can overcome the pitfalls of AI integration in an environment in which AI is increasingly common.

Increasing AI Interoperability and Data Sharing

To ensure alliances and coalitions are able to leverage AI technologies during their operations, states will need to remove barriers to data sharing and access. One initial step to enabling this type of interoperability is to establish formal agreements that govern the development and use of AI-enabled technologies and associated data. These formal agreements will not only prescribe procedures for collaboration, but help assuage fears that allies will renege on commitments.108 Agreements that explicitly define the responsibilities and expectations of member states help eliminate vagaries that otherwise allow a state to back out of commitments with partners.109

To integrate AI into alliance operations, policymakers will need to first establish how they will jointly develop and employ AI capabilities. This entails identifying the types of operations in which allies are willing to use AI-enabled technologies. Some states may only be willing to employ AI military systems in limited areas and eschew using AI for certain tasks. The U.S.-Singapore agreement, for example, stipulates that the two states will focus their AI efforts on humanitarian assistance and disaster relief operations.110 More narrowly scoped agreements that focus on noncombat operations may prove more palatable to policymakers and their domestic publics. These narrow agreements could serve as useful first steps to collaboration, but still yield lessons and best practices applicable across the full range of military operations.

Developing data-sharing policies and technical standards may be difficult given the sensitive nature of national security information and the variation in technical standards across alliance member states. Allies, however, have found ways to coordinate cooperation, even in sensitive areas. The United States and its Five Eyes partners — the United Kingdom, Canada, Australia, and New Zealand — have long maintained agreements that govern intelligence collaboration. The 1946 United Kingdom-United States Agreement, for example, established formal rules for sharing signals intelligence — intercepted electronic emissions and communications.111 The agreement spelled out how the states would cooperate on the collection, analysis, and dissemination of signals intelligence, while a technical appendix provided detailed technical and procedural guidance on communications intercept equipment and decryption and translation processes.112 Specifically, the agreement called on states to “make available to the other [states] continuously, currently, and without request, all raw traffic, [communications intelligence] end-product and technical material acquired or produced.”113 Some existing intelligence sharing agreements might allow for the exchange of the sensitive data needed to train and operate AI systems. When existing agreements are not in place or do not cover the types of data required for AI-enabled warfare, policymakers will need to develop new bilateral or multilateral agreements that enable interoperability and data sharing. These agreements and the procedures used to implement them will likely vary depending on the states involved and the degree and purpose of cooperation. In some cases, cooperation may be narrowly scoped to limited data sharing in support of a specific operation. In other cases, agreements may be far broader and cover issues related to research and development, interoperability, and extensive data sharing.

Even when formalized agreements establish the processes and institutions that enable AI cooperation between states, many leaders may remain hesitant to share the sensitive data that underpins AI development and operations. Information-sharing arrangements are plagued by commitment problems as states can back out of their agreements to exchange data if they fear that data will be leaked or their capabilities and shortcomings will be revealed.114 This might be particularly true in ad hoc coalitions or larger alliances, where relationships between member states may be weaker. Recent technological advances, however, may help overcome these commitment problems by convincing member states that their data will remain secure even when shared.

In particular, developments in the field of cryptology allow states to share data with partners for use in AI systems, while hiding the exact content of input data. Secure multiparty computation, for example, is a privacy-preserving technique in which AI algorithms perform their computations using an input that remains secret, but provide an output that is public to all authorized users.115 Secure multiparty computation has been increasingly used in the medical and financial sectors where analysts seek to assess trends but need to protect individual-level health and fiscal data to avoid violating privacy regulations.116 This and other privacy preserving approaches could be applied to a range of AI-enabled alliance military tasks, such as the classification of objects in satellite and reconnaissance imagery. Member states might feed sensitive intelligence data into a secure multiparty computation-based system managed by an alliance’s intelligence fusion center, which would then return information about potential targets, without revealing attributes about each state’s intelligence inputs.

To successfully integrate AI and share data, however, partners will also need to establish technical standards to ensure data is stored and formatted in ways that make it easily accessible to and usable by various alliance members. In designing these agreements, alliance policymakers might draw insights from existing state-level AI guidelines and alliance standardization protocols. The U.S. National Institute for Standards, for example, released its AI standards in February 2019. The guidance calls for defining data specifications that ensure AI technologies meet “critical objectives for functionality, interoperability, and trustworthiness.”117 In the alliance military context, this might mean ensuring that data associated with geospatial or signals intelligence are formatted and labeled in a common manner and stored on shared alliance networks. Or, it could mean establishing alliance-wide protocols for data security and integrity to minimize the risks of data poisoning. These specifications could be codified in formal arrangements like NATO’s standardization agreements, which provide standards for thousands of systems and processes ranging from aerial refueling equipment to satellite imagery products.118 These standards ensure “doctrine, tactics, and techniques are developed in harmony” to help allies “operate effectively together while optimizing the use of resources.”119

### 2AC---Unilat Fails

#### Alliances key to AI versus Russia and China---the US can’t do it alone

Andrew Imbrie et al 20, Andrew Imbrie Ryan Fedasiuk Catherine Aiken Tarun Chhabra Husanjot Chahal. Center for Security and Emerging Technology (CSET) at Georgetown’s Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. February. "Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI" //pipk

America’s broad network of allies and partners is a source of enduring strength. In an era of economic and technological competition with China and Russia, the United States benefits from allies that share its values and produce troves of strategic resources, including computer and data science experts; private sectors that are innovative, dominant and trend-setting; data on which to train AI algorithms; advanced microprocessors and data storage units; governmental research and development (R&D) investments; diplomatic support for initiatives in AI safety and governance; and the clout needed to export norms and best practices to the rest of the world.

Alliances matter in the AI context because they provide a framework for cooperation, data sharing, dissemination of best practices, joint planning, and procurement. The market adequately incentivizes some forms of cooperation, such as data labelling and exchanges. But alliances can help formalize and expand these relationships, correct for market failures in such areas as AI safety and security, coordinate development of use cases and risk assessments, enhance the legitimacy of international action, and validate the deployment of safe and reliable AI.

America’s alliances and security partnerships will shape the future trajectory of AI, even as AI reshapes the capabilities and operating environments for U.S. allies and partners. By investing in privacy-preserving machine learning and other techniques for improving the interpretability of AI systems, the United States and its allies can promote the development of AI consistent with liberal democratic values. Far-sighted investments could yield large dividends. AI has a wide array of applications that can benefit democracies, from improving data protection and privacy, to promoting transparency and accountability in government.

Advances in AI will also enable new military capabilities. Nations around the world use AI to enhance intelligence collection and analysis, streamline decision-making, lower operating costs, and improve military logistics through predictive maintenance. As China, Russia, and other authoritarian powers integrate AI with military capabilities, U.S. allies and partners will face a more complex operating environment. Advances in software and digital systems could render it more difficult to assess the balance of power in key domains. As the operational tempo of war accelerates, leaders might be tempted to integrate AI and machine learning into early warning and command and control systems, creating new risks and uncertainties for strategic stability.8 Competitors may rush to deploy AI-enabled capabilities without adequate testing, evaluation, verification, and validation. Compounding the risks, adversaries will seek to exploit vulnerabilities in AI systems and may even use AI to execute novel cyberattacks and disinformation campaigns aimed at undermining democratic institutions and sowing discord among the public.9

In meeting these challenges and seizing the opportunities that AI presents, the United States and its allies face tough trade-offs. Three, in particular, necessitate close coordination and prudent mitigation strategies.

First, the United States and its allies face a trade-off between capability and dependency.10 Showcasing a democratic way of AI will require the United States and its allies to pool resources, coordinate policies, and share best practices and information. Leveraging the capabilities of its allies and partners will amplify U.S. power and influence, but will also create inefficiencies and require compromise. While the United States can manage these challenges, it cannot eliminate them entirely—nor should it. As long as AI-related supply chains are global and AI talent both mobile and globally distributed, innovation in AI requires international collaboration.11 To excel in this new context, America will need to embrace its role as a “systems integrator” among like-minded allies and partners.12 Embedding cooperation in dense, decentralized networks plays to the United States’ strengths as a democratic power that favors market approaches to technological cooperation. By combining top-down vision with dynamic, bottom-up innovation and entrepreneurship, the United States and its allies can foster a competitive ecosystem that enables the best ideas to flourish.

These benefits should not obscure the risks. International networks can facilitate cooperation by creating focal points and enhancing the transparency and availability of information.13 As scholars have shown, however, networks of interdependence can also become the sites of competitive power plays, such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) financial messaging system.14 The United States has used SWIFT to counter terrorism, monitor illicit financial activity, and bolster the sanctions regime against Iran.15 At the same time, China is exploring alternatives to this U.S.-dominated cross-border payments system.16 Emerging competitive dynamics suggest the need for a strategic approach toward the development of AI, especially in semiconductors.

To manage the risks, the United States and its allies should pursue a range of mitigation strategies, including securing and enhancing their defense innovation bases and domestic economic competitiveness, diversifying partnerships in AI, investing diplomatic capacity in norms and standards for AI technologies and mobile telecommunications consistent with democratic values, and promoting flexible institutional configurations for partnership in AI.17

Second, the United States and its allies face a trade-off between competition and cooperation. All nations compete for relative military and economic advantage. In the age of AI, nations will also compete over whose vision of the future attracts the broadest support. Cooperation among democracies is necessary to guard against authoritarian uses of AI, but there are other imperatives for cooperative action. For example, democratic nations must cooperate with strategic competitors to ensure global economic stability and prevent misperceptions and miscalculations from spiraling into hostility; this could be achieved through arms control or international action to create norms and standards for emerging technologies.

Conventional wisdom suggests that the United States competes with China and Russia in AI and collaborates with allies and partners. While accurate, it is equally true that the United States competes with its allies and partners for top talent and resources in AI and must find ways to cooperate with China and Russia on AI safety and security, strategic stability, and crisis management to forestall the risks of accidents and miscalculations.18 When asked about obstacles to collaboration with the United States, for example, multiple officials from allied countries highlighted industrial competition as an impediment.

Cooperative dynamics are typically in pursuit of shared, global interests, while competitive dynamics tend to follow from a national calculation of AI’s impact on relative power and wealth. Researchers and scientists cooperate across national boundaries, but political leaders face difficult trade-offs between national interests and the international networks that foster open-source collaboration in AI.

Navigating these dynamics will require the United States and its allies to pursue a two-pronged strategy: expand areas for cooperation and competition that generate mutual benefits, while shrinking the space for competition that generates harmful effects or a race to the bottom. For example, the United States should manage competition within a rules-based framework that ensures a level playing field, protects intellectual property, and disincentivizes hidden government subsidies. At the same time, it should work with countries to discourage unfair competition that tilts the playing field in favor of state-backed enterprises, destabilizes financial markets, and triggers unforeseen disruptions to global supply chains.

The third trade-off is between safety and speed.19 This trade-off arises from the complex dynamics between the United States and its allies on the one hand, and strategic competitors such as China and Russia on the other. Artificial intelligence presents a range of opportunities and risks for the United States and its allies. AI systems are brittle and can fail accidently or behave unpredictably in real-world settings.20 American, European, Chinese, and Russian leaders increasingly view AI as a core element of national power. In an effort to gain comparative advantage, countries could rush to deploy untested or unsafe AI systems. It is in the interest of U.S. national security to pursue confidence-building measures in AI safety. It is also a core interest of U.S. allies: a majority of officials noted standards to ensure reliable and responsible AI development as a national AI priority and avenue for productive multilateral collaboration. By leading an international effort on safe and reliable AI, the United States and its allies can reduce threats to global security and promote strategic stability.

Policymakers could pursue any number of initiatives in this area, such as bringing together technical experts from the United States, China, and Europe to define shared concepts and standards for the robustness of AI systems; pursuing low-stakes joint projects to summarize the AI safety literature in different countries and promote transparency into applications of AI safety research; facilitating Track 1.5 and Track 2 dialogues on specific challenges in AI safety; or developing common standards and methods of testing, verifying, and validating AI systems, including AI-enabled safety critical infrastructure.21

### 2AC---Logistics Key---Say Yes

#### Allies will only say yes to the plan---logistics is non-controversial and leads to broader cooperation

Margarita Konaev & Husanjot Chahal 21, Research Fellow & Research Analyst, Center for Security and Emerging Technology, Georgetown University. "The Path of Least Resistance Multinational Collaboration on AI for Military Logistics and Sustainment" April. <https://cset.georgetown.edu/wp-content/uploads/CSET-Path-of-Least-Resistance.pdf> //pipk

The United States' global network of alliances and partnerships is a force multiplier in the strategic competition against China and Russia. With artificial intelligence as the focal point of this competition, fostering AI defense and security cooperation is becoming increasingly important. In fact, in its final report, the National Security Commission on Artificial Intelligence has recommended strengthening AI interoperability with U.S. allies and partners as a key element of building an AI-ready force by 2025.1 The AI future of the United States is then inherently intertwined with that of our allies and partners.

Although there are powerful incentives for multinational collaboration on AI, there are also nonnegligible technical, bureaucratic, and political barriers that could prevent like-minded nations from realizing a shared vision for the responsible use of military AI. This issue brief summarizes these challenges and then makes the argument that multinational collaboration on AI applications for military logistics and sustainment offers the path of least resistance. Our key takeaways are: • Multinational collaboration efforts on military applications of AI face an uphill battle. Public misgivings about the militarization of AI, tensions with Europe on questions of regulations and data privacy, lack of clarity regarding the best forum for collaboration, and technical challenges to ensuring that hardware and digital systems are interoperable and secure could impede efforts to work together. While no easy task, collaboration on AI-enabled technologies and applications related to military logistics and sustainment is technologically attainable, politically feasible, and strategically imperative. There are multiple pathways for collaboration on this set of technologies and applications, including joint standards for secure data sharing; collaborative research and development programs; multinational public-private partnerships; and joint military exercises that include AI-enabled logistics and sustainment technologies and capabilities.

As the Biden administration moves to implement its foreign policy agenda of rebuilding U.S. alliances and confronting China’s assertiveness, multinational collaboration on emerging technologies takes center stage. While not without challenges, joint projects centered on developing, maturing, and adapting AI applications for military logistics and sustainment offer both a viable and promising path forward.

### 2AC---Logistics Solves Norms

#### Momentum for democratic cooperation in AI building now---NATO logistic exercises key to preventing the US from leaving allies behind

Margarita Konaev & Husanjot Chahal 21, Research Fellow & Research Analyst, Center for Security and Emerging Technology, Georgetown University. "The Path of Least Resistance Multinational Collaboration on AI for Military Logistics and Sustainment" April. <https://cset.georgetown.edu/wp-content/uploads/CSET-Path-of-Least-Resistance.pdf> //pipk

Conclusion The idea of an international technology alliance grounded in a shared set of democratic ideals and ethical standards for the development and use of emerging technologies is gaining ground in the United States and among its allies and partners.75 Yet as the strategic competition between the United States and China intensifies, the United States may charge ahead in integrating AI into its military systems while allies trail behind. The growing gap in military and technological capabilities, in turn, could undermine interoperability and threaten the long-term viability of multinational coalitions like NATO and other key U.S. alliances.

While there are notable technical, bureaucratic, and political barriers to multinational cooperation in AI, especially for military purposes, AI applications for logistics and sustainment represent both a promising and critical area for collaboration between the United States and its allies. There are many ways allies can work together in this space, including by developing joint standards for data sharing, investing in collaborative R&D programs, advancing multinational public-private partnerships, and integrating AIenabled logistics and sustainment technologies into joint military exercises.

Depending on allies’ interests and capabilities, these efforts can take place within existing alliances, on a bilateral basis, or through a new and separate consortium dedicated specifically to cooperation on AI-enabled logistics and sustainment technologies. Working together with allies on this set of AI technologies will help advance shared security interests, promote interoperability, and ultimately, pave the path toward the ethical and responsible use of AI in military systems and mission.

#### NATO AI key to democracy---solves ethical AI---starting with non combat still solves

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

NATO has an interest, and a moral obligation, to promote the adoption of its values in the realm of AI. Democratic values inform the Alliance’s goals, thus giving meaning to its material capabilities – including its military power. At the same time, the integration of AI into the fields of security and defence poses unique moral, ethical, legal, and safety-related questions.85 It is thus imperative that the Alliance actively considers and operationalizes AI ethics, regardless of the degree and scope of AI integration within NATO and its Allies. The common principles and values pronounced in the Atlantic Treaty represent the foundations on which NATO was built. Such principles and values – democracy, freedom, rule of law, individual rights, free markets – are the bond underlying the transatlantic community, which in fact predates the Atlantic Alliance.86

Norms and values can strongly shape the international system.87 Given the intense international competition in the technological, military, economic, and normative domains, embedding democratic values into AI is as much a strategic imperative for the Alliance as it is a functional one.88 In addition to signalling to domestic populations that NATO and its Allies follow through on their commitments to uphold values as the basis of the political and military Alliance, incorporating AI ethics into the “NATO-mation” agenda also serves as a bulwark against the incursion of unwelcome illiberal values in the course of future technological development.89

It is worth noting that NATO’s role in the AI ethics sphere differs from that of many other organizations, such as national governments and the European Union, because NATO is not a regulatory body. NATO complies with existing laws and regulations, including the Laws of War, which nations and the international community created. This means that regulatory and normative questions such as the development and deployment of autonomous weapons systems will not be determined at NATO level. Nevertheless, there is still room for NATO to play a clear role. Indeed, given doubts and worries about the adoption of AI for military purposes, NATO can help generate more public support and engagement by clearly defining ethical boundaries and moral guidelines.

The uses of AI in military operations – ranging from logistics to maintenance, from recruitment to retainment, from intelligence, surveillance and reconnaissance to medical tests and medical evacuation, and more90 – go beyond the discussions on lethal autonomous weapons systems that have dominated European debate about AI in military affairs. Accordingly, the range of ethical questions relevant to NATO extend beyond focusing on the tip of the spear. Seemingly mundane uses of AI, such as in human resources or decision support, can still pose distinct ethical questions the Alliance should be prepared to handle. Addressing security risks,91 minimizing bias in systems,92 developing trust,93 and respecting privacy are fundamental tasks for the Alliance to ensure the future effectiveness of AI, whether in battle or in other functions.

The age of intelligent machines requires the Alliance to reiterate its commitment to values as new moral and ethical questions emerge, because algorithms do not have a conscience, personal preferences or moral agency. These statistical machines have no understanding of good and bad, or fair and unjust.94 All an algorithm can do is achieve its human-defined reward function, not provide any context or information on whether the right question is being asked.95 Instead of giving moral agency to algorithms, humans and organizations can view AI as a “moral entity”. This means that we humans are dutybound to adhere to our moral code of conduct when interacting with the systems, rather than shirking human responsibility to computers.96 At the organizational level, this means that the design, development and deployment of AI should be “ethically aligned” with the Alliance’s values and goals.97

This is important because AI is data-intensive, unpredictable and brittle.98 While a system may work well in the context in which it was trained, it may break in an unfamiliar setting. The reliance on BD in the current second wave of ML also creates fallibilities,99 given that the algorithms can scale up harm if the data over- or under-represents certain groups.100 For neural networks in particular, it may be impossible to explain or interpret results. Some refer to this as the “black-box” problem, meaning that the outcomes of these complex AI systems are opaque to humans that either want to reproduce the good, or prevent the bad from recurring. While traditional software can be debugged to solve a performance issue, the lack of linear causality between a programmer’s inputs and the AI system’s outputs means that it is difficult to track bias and reliability. Creating organizational processes to minimize these concerns across the AI lifecycle is critical to responsible use of the technology.

### 2AC---Solves China---NATO key to P3s

#### NATO is key---experimentation establishes standards that allow for interoperability and private-public partnerships key to winning the race in AI

Sonia Lucarelli et al 21. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

Another topical issue is the private-public partnership on AI. This is key in the AI race between the US and China – possibly leading to disadvantages for Allies vis-à-vis China – and in the relations between NATO and major civilian companies working on AI and Big Data. There is also the fundamental need to ensure interoperability in a fragmented scenario in terms of the Allies’ adoption of AI technologies. NATO has historically been an important player in the processes of standardization and could be such also in this case. In this context, some creativity may be needed: for instance, should NATO provide cloud computing services, namely enablers, the same way it provides air-space management or ground surveillance? Could the Alliance envision an integration of nationally-owned AI assets as it does for the integrated air and missile defense? These are important questions which, however, highlight the fact that defense is a sovereign issue and most decisions are taken by national governments, not by NATO as such.

The Alliance could play a prominent role in the AI domain. For instance, NATO could establish an AI champion to help Allies understand, adopt and integrate AI. Such champion could start with small projects aiming at validating the effectiveness of the solution, and then it could help Allies in training. A key, related issue in this regard is education and training. Similarly, the importance of wargames, simulations and experimentations is going to grow, and NATO has a role to play here, as the unique avenue to convene allied military and political bodies.

### 2AC---Benchmarks key to Interoperability

#### Testing is key---establishes standards for interoperability and data-sharing

Andrew Imbrie et al 20, Andrew Imbrie Ryan Fedasiuk Catherine Aiken Tarun Chhabra Husanjot Chahal. Center for Security and Emerging Technology (CSET) at Georgetown’s Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. February. "Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI" //pipk

Interoperability is a critical lubricant for U.S. alliances. To operate effectively, allies need to plan, train, and exercise together. Joint operational concepts, common doctrine, and compatible military capabilities and systems are required to communicate effectively and achieve shared objectives.66 As countries integrate AI into military systems, the United States and its allies must ensure that hardware and digital systems are interoperable and secure.

The United States and its allies could start with common standards for interpretability, safety, and security of AI systems, including AI-enabled, safety-critical systems.67 For AI-enabled military systems expected to perform a given function, the United States and its allies should agree on common benchmarks for accuracy and performance based on the same training and testing data. The CSET survey suggests that allies and partners desire such benchmarks, with a majority of surveyed officials expressing the need for international coordination and management of AI military applications, specifically autonomous weapons systems and unmanned vehicles for submarine detection. A German representative stated that collaboration with the United States would be enhanced by an AI strategy that includes a focus on AI-related defense and security threats.

The United States and its allies should also consider wargaming and table-top exercises to explore how sharing selected government data sets could shore up defenses against counter-AI techniques and other efforts to exploit the vulnerabilities of AI systems. Specifically, they should explore how sharing militarily relevant data sets and certain AI algorithms could help allied countries better test system robustness, expose mutual vulnerabilities, accelerate development of countermeasures, and establish common standards for testing, verification, and validation.68

The United States and its allies should define common standards for the level of robustness required for a given operation. Common defense planning and capability development in NATO and the EU should give priority to investments in AI safety and security, as well as common verification procedures for AI-enabled, safety-critical systems.

## AT Kritiks

### 2AC---AT: Securitization

#### Evaluate securitization by weighing the truth claims of our advantages and the ability of our plan to solve---our framework solves the impacts to securitization better than theirs---securitizing objective threats to democracy is good

Rita Floyd 11, Department of Politics and International Studies, University of Warwick. “Can securitization theory be used in normative analysis? Towards a just securitization theory” Security Dialogue 42(4-5) 427–439 //pipk

The project of establishing a list of criteria that can be used to determine the moral rightness of securitization should be seen as related to work in just war theory, where a list of criteria is used to determine the morality of war. Indeed, some of my criteria are very similar to those proposed by just war theorists. My appropriateness-of-response criterion, broken down into measured response and sincerity, for example, can be found in many writings on just war, while my requirement for the existence of an objective existential threat is comparable to the criterion of just cause. This suggests that certain things that hold true for just war theory could also apply to a just securitization theory. At the very least, they can be used to argue the case in favour of such a theory, while they also suggest what kind of criticisms might be levelled against what is attempted here.

The greatest success of just war theory – at least in the West – is that it has come to inform the practice of war, as decisions about war and how to fight it are made with reference to that theory. In Michael Walzer’s (2002: 933) words, ‘Moral theory has been incorporated into war-making as a real constraint on when and how wars are fought.’ A related positive consequence has been that just war theory has helped democratize war-making, insofar as citizens that are well versed in the ideas of a just war can and repeatedly do hold decisionmakers accountable for their actions. The outcry of the British public over the 2003 Iraq war serves as a useful example.

All this could hold true for a just securitization theory. Not only does such a theory promise to morally constrain securitization, making its occurrence less likely, but also general knowledge of such a theory could help to democratize the process of securitization itself. Both results are desirable because, like war – and regardless of what analysts might wish – securitizations are a recurrent feature of international relations, and the abnegation of moral reflection on securitization is simply not an option (see Rengger, 2002: 363). With this in mind, I will now discuss my three criteria in detail.

Objective existential threats Objective existential threats are threats to the existence of actors and orders regardless of whether anyone has realized this. To give an example, suppose I am exposed to lethal levels of radiation in an area where radiation levels are not normally checked, which leaves my exposure undetected. Given that I can neither smell nor see radiation, I am unlikely to be aware of it, yet my obliviousness is not going to save my life.

Objective existential threats become matters of security, and therefore ‘security threats’, only when a powerful actor frames and responds to them as such. Importantly, not all objective existential threats become security issues: Some are treated as health issues, others as police matters, and some may well be ignored. The reverse also holds, and not everything that is securitized necessarily refers to an objective existential threat; some security threats refer to perceived threats only.

Securitization can be justified as the right thing to do only if it refers to an objective existential threat. This is because the killing of innocent persons (directly or as ‘collateral damage’) that might well be an extraordinary measure resulting from securitization cannot be morally justified unless there is an objective existential threat. Once again, the storm that has erupted over the 2003 Iraq invasion is a case in point. Here, precisely the fact that lies about the existence of weapons of mass destruction artificially heightened the acuteness of the threat renders the whole endeavour and its consequences morally untenable.

How, then, can we find out whether a securitization refers to an objective existential threat or merely to a perceived threat? First, we need to figure out whether the aggressor really intends to destroy a given referent object. Second, we need to examine whether or not the aggressor has the means (capability) to do so.4 It should be clear that both of these conditions will have to be met at the same time.5 In the absence of any intention to harm A, the capabilities of B pose no danger to A. And the absence or lack of capabilities amounts to the same as insincerity. Insincerity in turn renders the threat non-objective.

In line with my revision of securitization theory, outlined above, I propose that just as we can get at the intentions of securitizing actors, we can get at the intentions of aggressors by comparing what they say with what they do. And, by ‘doing’ I mean a relevant behavioural change made by the aggressor, or by some entity instructed by the aggressor, in response to the threat. Discrepancies between what aggressors say and the actions they subsequently take to follow through on a threat are vital, as they suggest insincerity.

Having assessed the intentions of aggressors, we need to continue by assessing their capabilities. Within a state-centric context, traditionalists have made advances that are instructive for our purposes. Zeev Moaz (2009), for example, assesses capabilities by examining the level of manpower an aggressor has available for military service, along with its weapons capability, military budget, population size and political capacity to mobilize for national security. Capability assessment is easier in the context of the state, where data are more freely available, including from independent sources. In a non-state context, however, the analyst will have to try to figure out things such as the size of the aggressor (how many people subscribe to the cause), what the aggressor has done in the past, what kinds of states/organizations it is friendly with, and what we know about the latter.

To illustrate how we might proceed, let us consider the case of Al-Qaeda and whether it poses an objective existential threat to civilians in the West. Like most terrorist organizations, Al-Qaeda’s leadership has never made a secret of its intentions, having called on all Muslims to kill all Americans and their allies in order to liberate Islamic countries (Bin Laden, 2006: 296). A series of bombings/attacks provides conclusive evidence that they are sincere, as their words are matched by actions. These attacks also leave us with ideas about the organization’s capabilities: not only do they show ingenuity insofar as Al-Qaeda has transformed conventional means (passenger airplanes) into weapons, they also show that the organization’s biggest capability consists of human beings prepared to die for the cause. To summarize, as long as Al-Qaeda’s intentions do not change and as long as they are able to recruit new potential suicide bombers, they constitute an objective existential threat to at least some civilians in the West.

Objective existential threat analysis is not easy. Importantly, discourse analysis of publically available texts alone may not suffice here; instead, researchers might have to conduct interviews with relevant people and, if possible, analyse documents that are not in the public domain.6 Given this, it will be much easier to judge the morality of securitizations with hindsight, when information tends to be more freely available.

Legitimate referent objects My second requirement for moral securitizations is that the referent object of security is morally legitimate (hereafter legitimate). Inspired by consequentialism, I hold that a referent object of security is legitimate only if it is conducive to human well-being.7 This is based on the humanistic principle that holds ‘that the explanation and justification of the goodness or badness of anything derives ultimately from its contribution, actual or possible, to human life and its quality’ (Raz, 1986: 194).

Note that rather than subjective levels of ‘happiness’ or ‘life satisfaction’, I am interested in objective levels of well-being. In Amartya Sen’s terminology, my concern is with a person’s freedom (capabilities), which leaves them in a position ‘to promote or achieve objectives they value’ (functionings) (Alkire, 2002: 4). What matters, in short, is the capability to flourish.

There is, however, no consensus among the many people who have devised lists of capabilities/ human needs/human values (see Alkire, 2002: 78–84). But, it seems to me that different human needs (the term I prefer) are either more or less basic to well-being. Among the most basic of all human needs is the one that enables us to function as humans (Doyal and Gough, 1991). But, what is it to be human? James Griffin (2008: 32) offers a convincing answer when he suggests that what makes us human, and thus different from other sentient creatures, is the ability to make autonomous decisions: Human life is different from the life of other animals. We humans have a conception of ourselves and our past and future. We reflect and assess. We form pictures of what the good life would be…. And we try to realise these pictures. [Our status as human beings] centres on our being agents – deliberating, assessing, choosing, and acting to make what we see as a good life for ourselves.

Importantly, however, autonomy is not exclusively internal to the agent. Rather, different political regimes and structures are more or less good at encouraging and fostering autonomous behaviour (Doyal and Gough, 1991). Joseph Raz (1986: 391) puts it as follows: a person lives autonomously if he conducts himself in a certain way … and lives in a certain environment, an environment which respects the condition of independence, and furnishes him with an adequate range of options. In other words, in the absence of the necessary options I cannot lead an autonomous life, which is why autonomy is not only what makes us human but simultaneously a basic human need that must be satisfied if the objective is well-being.

The two ideas that have contributed most to providing individuals with options and therefore autonomy are liberal democracy and human rights. The latter foster autonomy by their very nature: they are based on the principle of the equality of all people, which entails that everyone is entitled to live a life of their own choosing, provided of course that this life does not infringe upon anyone else’s life choices (Donnelly, 1998: 44). It is also widely acknowledged that liberal democracy is intimately connected with autonomy, as liberal democracies are inseparable from certain individual liberties, including the right to free speech and the right to vote (Waldron, 2002; see also Dahl, 1998; Raz, 1986).

Such normative arguments are backed by empirical evidence, as it has been conclusively shown that liberal democracies generally do better than non-democracies in terms of providing people with the conditions and options that foster autonomy, including education, physical security, meaningful employment and economic security (Przeworski et al., 2000; Doyal and Gough, 1991). It is, hence, possible to argue, for example, that none of the North African states experiencing popular uprisings in the spring of 2011 qualifies as a legitimate referent object of security, precisely because those uprisings have been based on demands for democracy, economic security and respect for human rights.

To summarize, the moral rightness of securitization is in part a function of the legitimacy of the referent object, and legitimacy in turn is a function of the referent object being conducive to human well-being. Well-being is highest and most sustainably ensured in liberal democracies and when actors endorse human rights. The presence of liberal democracy and the honouring of human rights therefore serve as helpful indicators of human well-being in any given context.

Appropriateness of response The distinguishing characteristic of securitization is that it justifies the breaking of established rules and regulations in an effort to ensure the referent object’s survival. To achieve the desired goal, the emergency measures taken may even be extraordinary in nature. If our concern is with the morality of securitization, however, even the response to objective existential threats is not free from requirements. There are two such requirements: The first is that the degree of response must be measured to the threat in question. Not even the existence of objective existential threats automatically justifies a response that is equal to the action of the aggressor in both means and degree. A response is measured if it takes account of the capabilities of the aggressor. Depending on those capabilities, a measured response could be either more severe than the initial attack/threat or less so. One example of a measured response was Operation ‘Deny Flight’, when the UN Security Council imposed and NATO enforced a no-fly zone to protect civilians from aerial bombings during the Bosnian war (1992–5).

The second requirement is that the response must genuinely aim at addressing the threat. The securitizing actor must seriously intend to secure the referent object they themselves identified. Securitization does not necessarily benefit the referent object but can instead benefit the agent, as when the securitizing actor uses securitization to further his or her own ends with no intention of safeguarding the referent object of security (Floyd, 2010). We can test for the intentions of securitizing actors by examining whether or not a securitization is consistent in its own terms. This is done by comparing and contrasting what a securitizing actor says about a particular threat (securitizing move) with what they do in response to that threat (security practice). The securitizing actor is sincere only if the response matches the securitizing move. An example where this was not the case is provided by US environmental security policy under the Clinton administrations. The administrations indentified environmental security threats as acute, yet what was done in the name of environmental security barely addressed any of the threats. Indeed, the real beneficiary of such policies was the US national security establishment, not the American people, which was the stated referent object of security (Floyd, 2010: 118).

#### No internal link from our securitizing move to securitization by the state---we’re policy analysts, we can’t securitize---our framework for links solves political efficacy of securitization---no discourse links, our speech act is a normative argument as part of policy analysis and doesn’t actually cause securitization

Rita Floyd 11, Department of Politics and International Studies, University of Warwick. “Can securitization theory be used in normative analysis? Towards a just securitization theory” Security Dialogue 42(4-5) 427–439 //pipk

Postulating what we should be worried about is certainly one way of conducting normative security theory. Yet, there are other forms of normative analysis, and in this article I am offering a set of criteria that permit the analyst to evaluate whether a particular securitization is or was morally right/justifiable. Inspired by just war theory, where it is argued that, among other criteria, a just cause and the right intention determine the morality of war, I argue that there are three criteria that determine the moral rightness of securitization: (1) there must be an objective existential threat, which is to say a threat that endangers the survival of a an actor or an order regardless of whether anyone has realized this; (2) the referent object of security must be morally legitimate, which is the case only when the referent object is conducive to human well-being defined as the satisfaction of human needs; and (3) the security response must be appropriate to the threat in question, which is to say that (a) the security response must be measured in accordance with the capabilities of the aggressor and (b) the securitizing actor must be sincere in his or her intentions. I argue that a securitization is morally right only if all three of the above criteria are fulfilled at the same time. I also argue that a securitization theory complemented by a normative extension of this type would enable analysts to hold securitizing actors accountable, which would render the theory more policy relevant than is currently the case.

It is, however, not possible to extend the Copenhagen School’s original version of securitization theory by the aforementioned three criteria, as that theory precludes objective threat assessment and the School rejects the theorization of securitizing actors’ intentions. In short, original securitization theory cannot be used in normative analysis in the exact way suggested in this article; rather, my three criteria represent a further development of the revised securitization theory that I have developed elsewhere (Floyd, 2010). Given that it will feature as part of the argument set forth in this article, it will be useful to briefly recite my revision here.

My revised version of securitization theory was informed by the central insight that a securitization cannot simultaneously operate as an illocutionary speech act and be dependent on the speech act’s acceptance by the relevant audience, because the illocution denies a meaningful role for the audience (Balzacq, 2005; Stritzel, 2007). My solution to this conundrum was to bracket the audience from the securitization process.1 This can be done because the audience is not an analytical concept, but rather a normative concept in analytical disguise, which is to say that it does not stem from actual empirical observation of how politics operates but rather from Ole Wæver’s view of how politics, including security policy, should be done (Floyd, 2010: 50). Moreover, the idea that securitization operates like an illocutionary speech act also conflicts with the distinction often made by members of the School between a securitizing move and a complete securitization, because if it is ‘the utterance itself that is the act’ (Buzan et al., 1998: 26) then the speech act is tantamount to the complete securitization and any distinction redundant. In an effort to uphold this distinction, I suggested that it is not securitization that is an illocution; rather, it is the securitizing move alone that is the illocutionary speech act part of securitization. I argued that by framing an issue in security mode (in terms of an existential threat and a point of no return), the securitizing actor does something insofar as he or she issues a warning to the aggressor and/or promises protection to the referent object of security. A securitization is complete only if the warning/promise made in the speech act is followed up by a change in relevant behaviour by a relevant agent (the securitizing actor or someone instructed by the same) that is justified by this agent with reference to the declared threat. I called this second step security practice. My revised securitization theory thus holds that securitization = securitizing move + security practice (Floyd, 2010: 52–4)

One advantage of this revision is that it makes it possible to examine whether a securitizing actor is sincere. That is, do particular actors really intend to safeguard the referent objects of security they have themselves identified or did they securitize the given objects for different reasons altogether? The key to uncovering sincerity is to examine whether the rhetoric of the speech act is matched by subsequent security practice. Otherwise inexplicable discrepancy suggests insincerity,2 while continuity suggests sincerity.

Another advantage is that my revised securitization theory rejects the idea that language has securitizing force. Consequently, under my framework, the analyst remains functionally distinct from the securitizing actor at all times, including when he or she performs a securitizing move, which amounts to nothing more than a warning.3 And, while it is of course possible that a security analyst can convince decisionmakers of his or her opinion, even this does not make the analyst synonymous with the securitizing actor, because under my framework securitization exists not at the point of the speech act but only when a relevant actor changes his or her own behaviour in response to the existential threat justification. With the analyst not involved in securitization every time he or she makes a normative argument, my revised securitization theory offers a better starting point for normative analysis than the original formulation.

Although my revised securitization theory rivals original securitization theory insofar as it builds on a different understanding of what securitization means, it too aims to enable analysts to examine the process of securitization. In short, it too is an analytical security theory. The just securitization theory proposed here, however, is altogether different: it is a normative theory that aims to enable analysts to judge the moral rightness of any given securitization.

While the three criteria I propose are incompatible with original securitization theory, the idea of developing criteria by which securitization can be judged is not. This is the case because what I propose retains the functional distinction between the securitizing actor – the actor who makes the decision on what is securitized – and the security analyst – who merely sets the criteria for when an issue is securitized. If the securitization analyst can set criteria for the existence of securitization and its success, there is no reason why he or she should not also be able to set criteria that determine the moral rightness of securitization.

#### Only our framework determines the ballot---their kritik without our criteria is just an FYI---securitization analysis solves better than desecuritization

Rita Floyd 11, Department of Politics and International Studies, University of Warwick. “Can securitization theory be used in normative analysis? Towards a just securitization theory” Security Dialogue 42(4-5) 427–439 //pipk

Another more general critique that could be advanced against what is proposed here is that a normative extension of securitization theory confuses the aim of original securitization theory, which is to enable analysts to examine how securitization plays out in practice. While the latter is indeed quite different from what I am trying to achieve here, it is also the case that my argument sits neatly within a wider ‘securitization studies’, the realm wherein the securitization theorist can move from merely observing what is going on to making normative recommendations (Taureck, 2006: 59–60). The latter is desirable because it may not always be satisfying to end one’s analysis without a word regarding the moral rightness of the securitization one has spent (often considerable) time researching. In any case, having an informed opinion on the rightness of a political decision is better than silence, which could be mistaken for approval.

There are reasons to believe that the Copenhagen School would concur with such a view. This is most clearly evinced by the fact that they do not feel obliged to agree with all or any securitization. Indeed, ‘one of the purposes of [the securitization] approach should be that it becomes possible to evaluate whether one finds it good or bad to securitize a certain issue’ (Buzan et al., 1998: 34). This suggests that although the School’s view of security politics is considered ‘neutral’ (Buzan and Hansen, 2009: 38), normative evaluation is considered desirable, even necessary, and indeed a normative preference can be found in most of its members’ writings.

A key reason why this is the case is that under securitization theory language is believed to have securitizing force, which is to say that the securitization analyst simply by writing or speaking about security brings about securitization (Huysmans, 1999). The latter is problematic for the analyst, given that securitization can be abused by ethically undesirable groups. It is only natural that the securitization analyst will want to distance him- or herself from furthering the causes of such groups, and that can be done only by making a normative statement about the securitization in question. Members of the Copenhagen School do this by challenging all securitizations as negative developments, because in their view securitization leads to de-democratization and potentially a multiplication of the number of security dilemmas found in the world. In response to such negative developments, the securitization analyst is meant to point out that securitization is always a political choice and that actors should solve their differences by ordinary political means. In short, the School advocates desecuritization, the process whereby formerly securitized issues move back into the sphere of normal politics, where they are dealt with by ordinary measures once more.

Objection 5: Desecuritization is an appropriate normative strategy The Copenhagen School’s preference for desecuritization, however, is somewhat more nuanced than the previous section might suggest. After all, its members hold that desecuritization is better only ‘if all other things are equal’, while they also recognize that this is not often the case and that the mobilization power inherent in securitization can be used for good ends (Buzan et al., 1998: 29). Nevertheless, these important qualifications do not change the fact that on a level playing field desecuritization is the School’s preferred option.

I take issue with the claim that desecuritization is better in principle for two reasons: first, desecuritization does not necessarily lead to politicization (Floyd, 2010: 57); second, from a moral point of view, ‘desecuritization as politicization’ is not necessarily preferable to ‘desecuritization as depoliticization’ (Floyd, 2007: 343n56).

Desecuritization as a normative strategy is problematic for yet a third reason. Informed by the observation that there are no objective security threats, desecuritization as a normative strategy works by depriving securitizing actors of the ability to ‘hide behind the claim that anything in itself constitutes a security issue’ (Buzan et al., 1998: 34). Accordingly, why should actors be allowed to turn anything into a security issue if it can be shown that there are no security threats per se, and that all security threats exist in the securitizing actor’s own head (and, later, in the heads of the relevant audience)? The Copenhagen School’s preoccupation with security operating in this way and no other, however, has left its members blind to the fact that while there may be no objective security threats, there still exist objective existential threats (see Balzacq, 2005: 181). Consequently, they cannot see that a securitization that refers to an objective existential threat is distinct from one that refers to a perceived threat only, and that some such threats are best addressed in security mode.

Conclusion It has been the aim of this article to develop securitization theory in such a way that securitization analysts can normatively evaluate securitizations without assuming the role of the securitizing actor and without postulating what we should be worried about. I have argued that setting criteria that determine the moral rightness of securitization is akin to the Copenhagen School setting criteria that determine both the existence of securitization and its success.

I have further argued that the strict confines of the Copenhagen School’s version of securitization theory necessitate a move away from this original securitization theory to a revised version that holds that securitization = securitizing move (existential threat justification that amounts to no more than a warning or a promise) + security practice (a change of relevant behaviour by a relevant agent that is justified by this agent with reference to the declared threat). The revision was necessary because, in order to examine the moral rightness of securitization, the analyst must: (1) establish whether or not existential threats are objectively present; (2) examine both the intentions of aggressors and those of securitizing actors; and (3) identify universal values that determine the referent object’s moral legitimacy. Members of the Copenhagen School would be deeply uncomfortable with all parts of this analysis, as they go against some of the fundamental principles and beliefs underlying original securitization theory, as well as some of the intellectual ancestors of the theory (see Floyd, 2010: 9–23).

I have also argued that a just securitization theory of the kind proposed here renders securitization theory more policy relevant, and that such a theory has the potential to democratize the process of securitization. But one look at the many writings and further theorizations of the role and nature of the audience suggests that such democratization is deemed desirable by many scholars working on securitization theory.

Beyond this, I would also suggest that a just securitization theory has implications for security studies more generally. Securitization theory has established itself as one of the most influential non-traditional security theories in existence. The idea that security is a self-referential practice, the related rejection of objective threat assessment, and not least the preference for desecuritization have meant that securitization theory is often classified as part of the post-structuralist end of critical security studies, yet in its original formulation the theory is conceived as a third way between critical and traditional security studies (Buzan et al., 1998: 203–12). Notably, at its less extreme end, critical security studies includes objectivist formulations of security – for example, the one proposed by the Welsh School. A just securitization theory invites both traditionalists (because of the inclusion of objective existential threats) and those at the moderate end of critical security studies (the Welsh School’s concept of emancipation is similar to my formulation of human well-being as satisfaction of human needs)11 back to the table, making securitization theory attractive to a wider audience. Whether any of these theorists will become interested in the ideas of securitization theory remains to be seen; for certain is that just as just war theory is increasingly complemented by arguments for postwar justice (jus post bellum), a just securitization theory will have to be complemented by criteria that determine just desecuritization.

### 1AR---AT: Securitization

#### Solves runaway securitization by the state

Rita Floyd 11, Department of Politics and International Studies, University of Warwick. “Can securitization theory be used in normative analysis? Towards a just securitization theory” Security Dialogue 42(4-5) 427–439 //pipk

Just war theory has attracted both endorsement and criticism. One of the most pertinent criticisms is that it moralizes war, making it easier to fight. In the light of the ‘war on terror’, Anthony Burke (2004: 330), for example, has argued that ‘moral discourses [including just war theory] are part of the warrior’s political armoury; they are part of war’s machinery, not a rod in its wheels’. A similar objection could conceivably be advanced against a just securitization theory. It might be argued that such a theory moralizes securitization, making it easier to exclude and marginalize minorities and control populations. Some scholars already hold that securitization is a process of deliberate ‘insecuritization’. Didier Bigo (2001: 111), for example, has argued that security is in no sense a reflection of an increase of threats in the contemporary epoch – it is a lowering of the level of acceptability of the other; it is an attempt at insecuritization of daily life by the security professionals and an increase in the strengths of police potential for action.

I hold against this first objection that my criteria are robust enough to protect against the abuse of securitization. Note that the insecuritization argument has largely been advanced with a view to migrants in the European Union (Bigo and Guild, 2005; Huysmans, 2006); yet, crucially, under my framework even high levels of migration do not qualify as objective existential threats because the element of intentionality is missing. In the case of migration, we are not even dealing with a collective actor, but with lots of different people and their individual decisions. Intentionality would come into consideration only in the highly unlikely event that one state, perhaps after failing to provide for its own people, would urge or perhaps even pay its own people to emigrate en masse to another state. Under such circumstances, immigration might then become an objective existential threat to the receiving state.

#### Securitization framework---evaluate securitization debates using three criteria----1. Is the threat real, 2. Do we solve the threat and 3. Is the strategy we endorse non-escalatory

Rita Floyd 11, Department of Politics and International Studies, University of Warwick. “Can securitization theory be used in normative analysis? Towards a just securitization theory” Security Dialogue 42(4-5) 427–439 //pipk

While securitization studies have paid considerable attention to the moral value of desecuritization, they have paid almost no attention to the morality of securitization. In this article, I attempt to rectify that situation by proposing a revision of securitization theory that specifies three criteria that – if fulfilled at the same time – would render a securitization morally right. The criteria are: (1) that there is an objective existential threat; (2) that the referent object of security is morally legitimate; and (3) that the security response is appropriate to the threat in question. Although what is suggested here is considerably removed from the Copenhagen School’s original securitization theory, it is akin to that framework insofar as it retains the functional distinction between the security analyst and the securitizing actor. Indeed, the development of criteria that determine the moral rightness of securitization is analogous to the Copenhagen School’s devising criteria that determine both the existence and the success of securitization.

## AT: Topicality

### 2AC---Security Cooperation

#### Security cooperation is one of these 11 things---we’re testing and evaluation

Michael J. Mazarr et al 22, senior political scientist at the RAND Corporation. "Security Cooperation in a Strategic Competition" Research Report. <http://www.rand.org/t/RRA650-1> //pipk

To pursue this analysis, we first had to define the bounds of what we would assess. Official U.S. government definitions of security cooperation are very broad. One definition from the Defense Security Cooperation Agency states that security cooperation

comprises all activities undertaken by the Department of Defense (DoD) to encourage and enable international partners to work with the United States to achieve strategic objectives. It includes all DoD interactions with foreign defense and security establishments, including all DoD-administered Security Assistance (SA) programs, that build defense and security relationships; promote specific U.S. security interests, including all international armaments cooperation activities and SA activities; develop allied and friendly military capabilities for self-defense and multinational operations; and provide U.S. forces with peacetime and contingency access to host nations.3

Such definitions clearly include almost any security-related activity for any purpose. To scope the focus of the study, we reviewed official state documents and strategies and the literature on security cooperation to identify 11 types of activities: 1. military aid, which includes funding through the Foreign Military Financing (FMF) program, the Excess Defense Articles program, and other grants and loans 2. arms sales and transfers,4 such as U.S. arms sales through the Foreign Military Sales (FMS) and Direct Commercial Sales (DCS) programs 3. military capacity-building, such as U.S. activities under Section 1206 of the annual National Defense Authorization Act and Sections and 2282 and 333 of U.S. Code, Title 10 (the train and equip authority) 4. education and training, including international military education and training (IMET), professional military education (PME), and regional centers 5. personnel exchanges, such as U.S. activities under the Military Personnel Exchange Program and the State Partnership Program 6. military exercises, both bilateral and multilateral and those that involve foreign partners 7. access-related agreements, such as status of forces agreements (SOFAs) and agreements related to base access and information-sharing 8. armament-related agreements, such as those for co-development of systems and for research, development, test, and evaluation activities 9. sustainment of donor-nation equipment by the donor, the partner, or third parties 10. institutional capacity–building to strengthen the partner institutions that support security services 11. humanitarian assistance and disaster relief (HA/DR), which offers support for efforts to relieve suffering.

## AT: Counterplans

### 2AC---AT: Non-Mil CP

#### Defense cooperation key

Christie Lawrence & Sean Cordey 20, concurrent Master of Public Policy and Juris Doctorate 2024 candidate at Harvard Kennedy School and Stanford Law School and recipient of Harvard Kennedy School’s John F. Kennedy Fellowship. She previously worked as a management consultant for Oliver Wyman where she focused on regulatory risk and global data protection for financial institutions. She also worked at the Department of State. Her research with the Belfer Cyber Project includes AI policy, cybersecurity, US-Russian cyber relations, and US foreign policy in the digital age. a dual Master degree in International Affairs candidate at the Fletcher School of Law and Diplomacy and the University of St. Gallen and was a Belfer Cyber Security Project research assistant. He previously worked for the Swiss ministry of foreign affairs in Washington D.C. and currently works as a researcher for the Cyber Defense Project at the Center for Security Studies (CSS) at the ETH Zürich. The Cyber Project Belfer Center for Science and International Affairs Harvard Kennedy School. "The Case for Increased Transatlantic Cooperation on Artificial Intelligence" August. <https://www.belfercenter.org/sites/default/files/2020-08/TransatlanticAI.pdf> //pipk

The US defense sector and the EU340 have separately recognized the importance of AI innovation and adoption. The Department of Defense’s 2018 National Defense Strategy recognizes the need for the Department to modernize its programs and address changing threats posed by new technologies like AI.341 The accompanying DOD Artificial Intelligence Strategy stressed that AI will change “the character of the future battlefield and the pace of threats” the US will face. Therefore, the AI Strategy outlined the need to develop and adopt AI to strengthen the DOD’s capabilities, enhance and streamline businesses processes through AI and ML applications, cultivate its AI workforce, engage with industry and allies to enhance capabilities and security, and lead in military ethics around AI.342 To lead defense-related AI efforts, the DOD created the Joint Artificial Intelligence Center (JAIC) in 2018 to: 1) accelerate the operationalization and adoption of AI across the DOD, 2) establish a “common foundation” to enable the DOD to scale AI’s impact, 3) coordinate the DOD’s AI priorities, and 4) attract and foster leading AI talent.343 The US has undertaken extensive AI and ML-related R&D and, as mentioned in the United States Government Funding section, defense-related AI R&D appears344 to be larger than non-defense AI R&D. For example, DARPA’s AI Next Campaign—launched in 2018—focuses on improving the security, robustness, and reliability of AI and ML while decreasing the required computing resources, while its Artificial Intelligence Exploration (AIE) funds academia and small industry for high-risk, high-reward projects.345

The EU is less advanced in developing an AI strategy for the defense sector. This broadly stems from its comparatively more nascent defense industry and differing opinions between EU Member States on AI’s defense applications. In 2017, the EU established the European Defense Fund (EDF) and the Permanent Structured Cooperation (PESCO) to bolster its security, defense industry, and strategic autonomy.346 EDF and PESCO, as Ulrike Franke, Policy Fellow at European Council on Foreign Relations explains, are vehicles to establish greater European defense collaboration, but these vehicles are not as developed or unified as other defense cooperative mechanisms or alliances like NATO.347 Furthermore, European Member States disagree about the role AI should play in the defense sector, with some countries extremely averse to the idea of developing lethal autonomous weapons systems (LAWS) given the trope of the “killer robot.”348

Joint US-EU defense-related AI efforts appear sparse,349 however there is a growing push particularly from the US and NATO to increase transatlantic defense cooperation on AI. The aforementioned DOD Artificial Intelligence Strategy stressed the importance the US and allied partners to “maintain its strategic position to prevail in future battlefields and safeguard a free and open international order.”350 Growing Chinese and Russia aggression and weaponization of new technologies like AI is a central motivation for the US government’s push to strengthen the international AI alliance.351 Acting Director of JAIC Nand Mulchandani explains that collaboration with European partners on AI is necessary for three main reasons. First, joint AI R&D and adoption efforts are important for developing strong capabilities and bolstering transatlantic hard power. Second, leading AI capabilities--among the US and its allies--acts as a deterrent for conflict. Third, if deterrence fails, AI-related interoperability and capabilities are necessary if the US and its allies must go to war. A military alliance cannot be lopsided and unequal AI adoption may hinder the tactical aspects of conflict.352 During the already mentioned recent visit to NATO headquarters in Brussels, Former Director of the JAIC Lt. Gen. Shanahan had collaborative engagements with European allies and NATO around the importance of AI joint efforts, ensuring military interoperability, and the convergence of Europe’s AI ethical principles with the DOD’s five principles of AI ethics.353 The visit appeared to increase NATO’s focus on devising an AI strategy for the Alliance.354 Despite these positive steps, there are still concerns about potential obstacles to increased defense collaboration, particularly around IP ownership and funding restrictions that may exclude US involvement in EDF and PESCO.355, 356

Overall, as noted in the US-EU roadmap for S&T, the volume and intensity of transatlantic scientific and technology collaboration has increased since the 1990s. Most notably, it has blossomed in areas where interests— whether strategic, societal, or economic—of both sides of the Atlantic overlap (e.g., in the health, environmental sciences, and energy sectors). However, in the case of AI there seems to be a large imbalance between the level, intensity, and volume of cooperation relative to the importance of AI. Indeed, both the US and the EU recognize AI’s transformative potential and share interests in its development and deployment. Yet transatlantic cooperation on AI is still its infancy—at least compared to other technological sectors. As a result, it has plenty of room to grow. Deepening this collaboration will not only require proactive efforts but also strategic endeavors to overcome the existing underlying challenges to collaboration.

#### Defense data sharing key

Christie Lawrence & Sean Cordey 20, concurrent Master of Public Policy and Juris Doctorate 2024 candidate at Harvard Kennedy School and Stanford Law School and recipient of Harvard Kennedy School’s John F. Kennedy Fellowship. She previously worked as a management consultant for Oliver Wyman where she focused on regulatory risk and global data protection for financial institutions. She also worked at the Department of State. Her research with the Belfer Cyber Project includes AI policy, cybersecurity, US-Russian cyber relations, and US foreign policy in the digital age. a dual Master degree in International Affairs candidate at the Fletcher School of Law and Diplomacy and the University of St. Gallen and was a Belfer Cyber Security Project research assistant. He previously worked for the Swiss ministry of foreign affairs in Washington D.C. and currently works as a researcher for the Cyber Defense Project at the Center for Security Studies (CSS) at the ETH Zürich. The Cyber Project Belfer Center for Science and International Affairs Harvard Kennedy School. "The Case for Increased Transatlantic Cooperation on Artificial Intelligence" August. <https://www.belfercenter.org/sites/default/files/2020-08/TransatlanticAI.pdf> //pipk

Rationale: High-quality, diverse data, as Acting Director of the JAIC Nand Mulchandani explains, enables better training and development of algorithms and reliable AI. The defense-sector (NATO) would benefit from diverse data collected by many countries. It is difficult to reduce the timeline to properly collect, organize, store, and develop governance mechanisms around data. Therefore, Acting Director Mulchandani explains, it is important for the US, the EU, and NATO to begin data-sharing efforts as soon as possible to prevent future obstacles.423 However, defense data-sharing efforts, as Ulrike Esther Franke explains, are difficult to initiate because of sensitivities around data, particularly around military operations. It may therefore be easier to establish data-sharing efforts centralized around solving a discrete question or achieving a specific goal.424

The US and the EU should remove obstacles to sharing defense and intelligence-related data where appropriate. They should also fund and prioritize addressing challenges to data sharing through NATO. Efforts should begin immediately as data sharing and governance projects are often lengthy undertakings. Projects focused on achieving a specific, concrete goal should lay the groundwork for larger-scale, general efforts.

#### Can’t solve the aff---defense cooperation is key to the alliance

Christie Lawrence & Sean Cordey 20, concurrent Master of Public Policy and Juris Doctorate 2024 candidate at Harvard Kennedy School and Stanford Law School and recipient of Harvard Kennedy School’s John F. Kennedy Fellowship. She previously worked as a management consultant for Oliver Wyman where she focused on regulatory risk and global data protection for financial institutions. She also worked at the Department of State. Her research with the Belfer Cyber Project includes AI policy, cybersecurity, US-Russian cyber relations, and US foreign policy in the digital age. a dual Master degree in International Affairs candidate at the Fletcher School of Law and Diplomacy and the University of St. Gallen and was a Belfer Cyber Security Project research assistant. He previously worked for the Swiss ministry of foreign affairs in Washington D.C. and currently works as a researcher for the Cyber Defense Project at the Center for Security Studies (CSS) at the ETH Zürich. The Cyber Project Belfer Center for Science and International Affairs Harvard Kennedy School. "The Case for Increased Transatlantic Cooperation on Artificial Intelligence" August. <https://www.belfercenter.org/sites/default/files/2020-08/TransatlanticAI.pdf> //pipk

Our assessment of existing transatlantic S&T cooperation and potential future applications of AI technologies has highlighted three sectors where US-EU collaboration on AI could be easily expanded. AI innovation and applications in the areas of healthcare, environmental sciences, and defense will be critical for the advancement of the “global good.”

Enhanced collaboration on AI in healthcare and environmental sciences will capitalize on existing S&T coordination and established research relationships.321 The benefits from pooling resources on health-related and environmental sciences will outweigh apprehensions from private sector competition or government. AI-related cooperation in the defense sector is key for the continuation of historical security alliances.

#### Perm do the CP---State department is topical

Michael J. Mazarr et al 22, senior political scientist at the RAND Corporation. "Security Cooperation in a Strategic Competition" Research Report. <http://www.rand.org/t/RRA650-1> //pipk

Congress authorizes DoD and the U.S. Department of State to work with foreign nations to conduct multiple types of activities that fall under the auspices of security cooperation. These activities range from arms sales and military exercises to educational courses and personnel exchanges. Each year, the United States spends billions of dollars and partners with thousands of foreign students and trainees on U.S. security cooperation efforts, which involve large numbers of active-duty and reserve military members, U.S. government civilians, and contractors who plan, execute, monitor, and evaluate these efforts. In some cases, partner nations fund the activities, and in other cases, the United States funds them in the form of loans and grants.

### 2AC---AT: Export Control CP

#### Export controls are bad---undermine innovation, can’t solve the case

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

Arms control. There have been various calls to adapt different types of arms control regime to AI. Reciprocity, monitoring and compliance pose key challenges here. How can we trust countries that have not complied with existing arms control regimes to respect new ones? How can we convince countries that do not want to enter existing arms control regimes to join new ones? Cooperation, political scientists note, is a matter of interest and trust: any control regime not built on these two pillars is doomed to fail.269 At this stage, it is difficult to find the political conditions conducive to either. There is, however, an additional problem.

Weapons or technology control? Lethal autonomous weapons are a type of military equipment which is hence subjected to clear and existing rules and regulations – both domestic and international – related to the sale, export and transfer of military technology. The key argument for banning lethal autonomous weapons, however, builds on a different logic: the dual-use nature of the constituent technologies favors its swift, and to some extent subtle, diffusion. In terms of inputs, the AI Inputs Triad is based on algorithms, data and microprocessors – although human capital should not be underestimated.270 Banning the weapons without underlying controlling the technology risks being ineffective, at best, and counterproductive, at worst, as it may increase the incentives to countries or actors to source key component technologies and undertake research on their integration so as to neutralize the effects of a ban.

Technology control regime. The above discussion on the dual-use nature of the AI Input Triad has led some to recommend tight control regimes on the export of AI-related technologies. While there is an obviously strong rationale for this line of thinking, its very ease of execution brings its own risks.271 NATO Allies admittedly have a strong interest in preserving international stability and preventing malicious actors from possessing capabilities that may be conducive to destabilizing activities. However, NATO Allies are in this position because of their technological prowess: any export control regime should therefore take into account the possible effects on the Allies’ industrial base and their longerterm implications. Were NATO Allies to lose their technological primacy, their political power – including the capacity to restrict the spread of sensitive technologies – would be undermined. In this respect, it is useful to divide the discussion into the component items conceptualized in the AI Input Triad – data, algorithms and processors.

### 2AC---AT: Civilian Tech CP

#### Market forces can’t solve the aff---corporate r&d can’t meet NATOs needs on their own

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

Commercial technology and public goods. A common theme in discussions about AI is the role of private industry. The story goes that the commercial sector is leading in innovation on AI, and that the defence establishment, in contrast to the Cold War, thus needs to adapt to the needs and capabilities of the private sector, rather than the other way around.240 While defence establishments would certainly do well to shed some bureaucratic deadweight that constrains them from following the “lean”241 or “agile”242 ways of the commercial sector, it is problematic to import private-sector assumptions and practices as this line of thinking suggests.243 Namely, market forces do not always and necessarily lead to the social optimum: markets sometimes lead to the under-provision of public goods such as national defence, because of the inherent difficulty of charging all potential beneficiaries. Similarly, markets may favour the overproduction of negative externalities like pollution, because producers bear only a tiny fraction of the total cost. We observe these dynamics of market failure when we look at AI-related R&D by private companies. First, corporate R&D generally has a narrow, short-term focus, to the detriment of broader, longerterm issues which are necessary for ensuring that AI yields positive returns in the distant future.244 Second, the computer intensiveness of ML is technically, economically and environmentally unsustainable.245 In particular, nobody has mastered how to properly size ML models and modern deep-learning algorithms are based on over-parametrization. This means their performance is inherently inefficient, in that they need an enormous amount of data and parameters. The cost comes in terms of computing resources. Realistically, existing trends are not sustainable.246 NATO and its Allies have operational and strategic incentives to promote leaner and greener AI. Operationally, there is a limit to the utility of computationally intensive AI systems “at the edge” – i.e., usage by small units in operations where connectivity is not assured.247 Strategically, correcting cases of market failure enhances technological prowess insofar as it means promoting broader, longerterm research on AI and the development of less computationally intensive solutions not only for ML, but also for other technological priorities such as quantum248 and aspects of biotechnology. Moreover, weaning ML models off massive training data is one measure of AI becoming more robust,249 and thus potentially less susceptible to data-driven biases.250 Procurement. R&D will, sooner or later, lead to procurement programmes. Transitioning AI into prevailing procurement paradigms, however, will not be immediate or easy. Defence procurement is particularly complex, given the range of strict requirements and specifications with which contractors have to comply.251 This is why traditional weapons manufacturers generally have an advantage when it comes to approaching defence buyers.252 AI, however, will entail a paradigm shift because the capabilities will continuously evolve. For AI-enabled autonomous systems in particular, as mentioned above, decision-making is “non-deterministic” and depends on the “dynamic environment” in which the system operates.253 This means that “traditional development and procurement approaches, based on full-path regression, are unfit”.254 This means that R&D also continues in the product deployment phase, as data and algorithms keep providing information and feedback that have to be integrated in order to achieve initial operational capabilities. Current “waterfall” procurement paradigms are set up so that engineers test prototypes according to defined specifications, and then subsequently move to production.255 With machine learning, the specifications will keep evolving as algorithms are fed new data.256 By extension, this means that testing cannot be treated as a singular phase prior to production and development. For NATO Allies, a more iterative procurement paradigm that does not depend on the sequential “waterfall” entails unique challenges. The integration of enterprise AI requires specific technical, legal, and organizational capabilities. This is linked to human-capital challenges in requirements, procurement and operations communities, as organizations leveraging AI “need their own people who know how to structure the problem, handle the data, and stay aware of evolving opportunities”.257 The development of AI-centred major weapon systems similarly calls for reform, or at least a remarkable adaptation, of defence procurement.258 Significant political, organizational and human capital will have to be invested. This is an additional reason why a centre such as the proposed A3IC could support the transition, through best practices, lessons learned and similar initiatives. Supply chain. Ben Buchanan has conceptualized AI inputs as a triad: algorithms, data and processors.259 Processors are the material part of the triad and they pose a key supply chain vulnerability.260 NATO as an organization has neither the capabilities nor the authority to strengthen the AI supply chain. Additionally, the supply chain is heavily skewed towards some Allies, like the US and Great Britain in semiconductors or the Netherlands in semiconductor manufacturing equipment, and partners, like Israel, South Korea and Japan – plus Taiwan, which is a close ally of several NATO countries.261 A useful exercise for the Alliance could be to make an assessment of the supply chain related to semiconductors. This is important for three main reasons. First, several Allies are conducting their own assessments, but an Alliance-wide picture is so far lacking.262 Second, as several countries consider semiconductors a strategic industry and thus aim at achieving a degree of selfsufficiency and autonomy, there is a real risk that different national strategies may collide, thus leaving the Alliance as a whole worse off. Last, but not least, such an assessment could be helpful in determining potential joint or common solutions, including arms control and export controls, as discussed in the next chapter, as well as coordination in R&D investments.

#### Civilian AI tech can’t solve---military specific cooperation is key

J.A.P. (Antoine) Smallegange et al, 18. Dr. H.J.M. (Harrie) Bastiaansen, A.P. (Auke) Venema MS, & Prof. Dr. A.W. (Adelbert) Bronkhorst. NATO Sience and Technology Board. "Big Data and Artificial Intelligence for Decision Making: Dutch Position Paper" //pipk

One of the main tasks of NATO is to facilitate military collaboration between member states. Traditionally, NC3O has focused on interoperability and on ways to support headquarters with C2-systemens to facilitate cooperation. The international trend of hyper connectivity and globalization in combination with the requirement of collaboration at tactical levels, make a shift towards interoperable support of tactical commanders paramount. STO can provide nations and NC3O with insights in new possibilities of emerging technologies to support the commanders.

Furthermore, technology for big data and AI is currently developing at a fast pace, with major potential impact on both the strategic, operational and tactical military decision making processes. As such, the military operational benefits may be huge and diverse. However, the full potential cannot (yet) be overseen and will have to be established over time. Moreover, these new technologies not only have potential benefits, but also short-comings and risks that need to be assessed, and for which possible mitigating countermeasures have to be identified.

Notwithstanding these uncertainties, it is now considered time to act within the NATO Research and Innovation community, so as to be well prepared for upcoming developments. Several advanced civil applications of AI have emerged over the last few years, and adaptation of these innovations is growing rapidly. Examples are autonomous vehicles, personal assistants such as Apple’s Siri, software for “predictive policing” and “cognitive computing” solutions such as IBM Watson [1]. But invariably these applications have restrictions. For example, personal assistants mainly act as voice-activated intermediary between web-based services and the user. Autonomous vehicles only perform optimally in uncluttered, ordered environments. Cognitive computing requires access to sufficiently structured big data and extensive (preparatory) work by experts to train the system and integrate different modules for e.g. reasoning, predictive modeling and machine learning.

For military applications, there are important requirements that may render civilian technologies unsuitable or demand changes in implementations. Systems have to work in a context that is highly unstructured and unpredictable, and with opponents that deliberately try to disrupt or deceive them. Ethical and legal issues will often play a major role. Hence, defense organizations have to make difficult choices because they must, on the one hand, benefit from the rapid civil developments while, on the other hand, choose wisely where to invest to make sure that applications will be fit for military use. Furthermore, the question is whether they are on the right track in enabling the trend/evolution towards big data and AI with their current developments of the data and IT infrastructures.

### 2AC---AT: Consult AI CP

#### NATO says no

Sonia Lucarelli et al 21. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

The AI Adoption in the Defense Domain and NATO’s Role. In discussing what AI will mean for allied militaries and the Alliance as such, a basic question should be addressed: is AI a technological revolution or is it an instance of technological evolution? Different pieces of evidence can support both interpretations. It would probably be hard for Allies, from a political perspective, to adapt swiftly to a rapid technological revolution. NATO approach, because of the consensus characterising its procedures, will have to be more evolutionary, granular and nuanced. In any case, it is unlikely to see in the next future AI making decisions for the North Atlantic Council (NAC) or the Nuclear Planning Group (NPG). There are psychological, cultural, organizational, political as well as technical reasons for this. The journey to AI is likely to be rather troublesome. Agile software development, for instance, enables the development of superior software but, at the same time, also calls for different procedures, organizational structures and processes, touching upon organizations’ identities, missions and culture.

### 2AC---AT: NATO PIC

#### NATO AI standards key to interoperability---aligns EU and DOD standards

Joanna van der Merwe 21, Fellow, Defense Tech Initiative. Center for European Policy Analysis. MA in International Relations and Global Conflict in the Modern Era, from Leiden University. She conducted her research in collaboration with the Land Warfare Centre of the Netherlands Ministry of Defence, focusing on Artificial Intelligence and the future of combat. This research built on her previous experience at the Netherlands Army looking at big data on the future battlefield. Joanna is currently the Privacy and Protection Lead at the Centre for Innovation at Leiden University. She has also worked on early warning systems for mass atrocities at the Signal Program on Human Security and Technology at the Harvard Humanitarian Initiative. She also continues to advise and speak on data and AI in contexts such as policy-making and the future of warfare and defence. February 17. "NATO Leadership on Ethical AI is Key to Future Interoperability" <https://cepa.org/nato-leadership-on-ethical-ai-is-key-to-future-interoperability/> //pipk

Establishing NATO ethical AI principles is the first step toward both technical and political alignment.

In October 2020, Deputy Secretary General of NATO Mircea Geoană highlighted the benefits of establishing a “transatlantic community cooperating on Artificial Intelligence (AI).” The Deputy Head of NATO’s Innovation Unit followed with a commitment to its responsible use. The US Department of Defense (DoD) adopted Ethical Principles for AI in 2020 and has committed to bringing together NATO member and partners to operationalize these principles. Despite these statements and developments, more work is required to tackle the very real challenge that ethical AI will pose to future interoperability within NATO.

Without a NATO-led initiative focused on aligning these ethical principles across the Alliance, the interoperability risk of nations fielding AI-based systems that hinder joint operations is high. As the foremost security framework for Europe and North America, as well as the leading defense alliance for promoting and protecting democratic values, NATO is able to facilitate alignment on this issue. As part of a broader strategy on emerging and disruptive technologies, NATO must prioritize ethical AI if it wishes to promote the shared values upon which it was founded, play a key role in facilitating innovation across the Atlantic, and ultimately retain the ability of its members to undertake joint operations.

Establishing NATO ethical AI principles is the first step toward both technical and political alignment, in turn enhancing and fostering interoperability, which is the foundation for NATO to respond to emerging threats as an Alliance, in a flexible and timely manner.

A key challenge for NATO is raising awareness that the answers to ethical questions can no longer be left to later stages of the development and procurement cycle. Decisions made at the political and legal level will have a significant impact on the engineering practices used to develop AI, as well as the technical characteristics of the AI-based systems. The answers to questions such as respecting human dignity, human control, and accountability will be the foundation upon which many technical elements are programed. Systems developers need to make a number of calls throughout the development cycle informed by the answers to key questions, including:

how to label data

what data to use, and

what is an acceptable outcome?

These answers will also impact how AI systems are evaluated and ultimately deployed.

If individual nations or groups are left to develop their own ethical principles without wider alignment to NATO, the result will be a number of AI-based systems with varying technical specifications based on the legal and policy decisions made by individual governments when answering the key questions. As has been demonstrated in areas such as facial recognition and policing algorithms, the assumptions made by those developing the tools and answering the key questions have a significant impact on the real-world functioning of the tool and societal acceptance of its ethics. The risk of tools failing to gain acceptance depends on the legal and ethical decisions made by governments. For the military, this may mean one state using an AI-based system that is seen as unacceptable by another, and in a joint operation one state fielding a system that cannot be used by another. Or worse yet, this could render a joint operation impossible. Without the ability to interoperate across NATO, the inability to effectively and efficiently respond to future threats would undermine the Alliance.

The role of the private sector is another aspect of ethical AI development that has proved a challenge to governments and the transatlantic relationship. Within states, governments have struggled to adequately regulate Big Tech firms, which has led to these companies encroaching on government responsibilities to protect and uphold the public interest. This encroachment permeates all aspects of government, including defense and security. As Deputy Secretary of Defense Kathleen Hicks discussed during her confirmation hearings, the lack of competition is also a challenge to innovation in the private defense industry. This, along with a lack of regulation, feeds into the power imbalance between the sectors. Consequently, private sector companies building the AI and AI systems that are or will be deployed on the battlefield are deciding the ethics policies for themselves.

The transatlantic partnership must focus on coordinating these core principles and systematic governance to ensure AI systems development aligns with the rule of law and democracy. In particular, this must ensure answering questions about human dignity, human control, and accountability. NATO is the ideal defense and security forum for this alignment. Given the US lead on adopting ethical principles for the entire DoD and the EU’s drive to assert checks and balances for private-sector tech companies, NATO remains the organization that can bring these two together and establishes the ethical bottom line. These will then ensure the diverging legal and ethical stances towards Big Tech do not lead to an interoperability barrier in the future. If developments surrounding the General Data Protection Regulation (GDPR) and the challenges it brought for U.S.-based, data-driven companies are any indication, a strong transatlantic led initiative is needed in order to ensure the same challenges do not hinder NATO.

The solution to the challenge that ethical AI poses for the future of interoperability within NATO is for the Alliance to establish shared transatlantic ethical principles, informed by the US DoD, the EU, and others. Establishing these principles will not only strengthen transatlantic political relations; more technically, it will allow for the establishment of standardization agreements and inform training and education initiatives of the Alliance in the future.

#### NATO key to standardization---solves innovation

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

Over the past 150 years, the complexity of technology – whether military or commercial – has grown exponentially.311 The fact that increasingly capable technologies developed in different countries, in different years and by companies operating in different industries can work together and interact efficiently is, to a significant extent, a product of standards.312 Standards are, literally, documents defining technical specifications, requirements, guidelines or characteristics.313 For instance, all USB sticks enter any USB port and our laptops or smartphones can connect to any WiFi network: this is the product of standards. By the same token, standards are intensively used in the military domain to address similar compatibility issues, from the measurements of cartridges to communications. Standards deserve attention because they are also going to play a key role when it comes to AI, ML and BD.

There are, fundamentally, two types of standards. Technical standards refer to specificities, parameters and characteristics. Non-technical standards define procedures, processes and practices. To examine this issue in greater detail, it is useful to look more broadly at what standards do and what their merits are. First, standards not only connect technologies vertically (in the same field) and horizontally (across different fields), but also span different times of development. In this way, standards enable innovation. A related point is that common standards also expand the size of a market, as they eliminate nontariff barriers and thus contribute to guaranteeing economic efficiency and technological effectiveness.314 Second, standards define and protect intellectual property and thus make it possible to gather royalties: in this way, they also incentivize innovation.315 In the language of social science, standards are thus an institution that makes it possible to solve a collective action problem related to adjudication of rents in complex systems.316 Third, standards also make it possible to comply with specific requirements. For instance, technical standards may require certain levels of safety and security through the imposition of specific parameters. By the same token, non-technical standards may call for procedures and processes that comply with these or other demands – for instance, emphasizing transparency or calling for specific verification steps.317

The above discussion highlights how, despite their technical nature, standards have an important political, economic and ethical dimension. Standards, however, also have an important military dimension, as the case of NATO highlights. Historically, NATO has played a critical role in standardization. As Paul Beckley notes, “with nearly 6,000 documents in its database, NATO is the most prolific international military standardization organization in the world”.318 Furthermore, standards are the backbone of interoperability – which, in turn, is the lifeblood of a military alliance. NATO collective capacity is, however, more than the simple sum of its parts, or “having the same missiles or tanks”.319 The emergence of AI, ML and BD highlights this point. As this new set of technologies are integrated into the economy as well as in countries’ armed forces, standards will provide a fundamental contribution. NATO has a key role to play here, both in ensuring a swift and risk-free technological transition through standards and in infusing its ethical and moral commitments into the new technologies.320

At least four main issues are important for the Alliance. Standards and ethics. NATO cannot lead and shape ethical discussions about AI if is unable to translate its ethical commitments into technology. The propagation channel to achieve this goal is constituted by technical and non-technical standards. However, in recent years, as Paul Beckley warns, NATO’s once robust standardization programme has lost vitality: since the early 2000s, NATO has developed few new standards and, since 2010, most have been doctrinal rather than technical.321 Additionally, while AI technologies evolve quickly, the standardization process may often be lengthy, and given its consensus-based nature, it can require significant time in large organizations. Key ethical values such as explainability, traceability or transparency need to be translated into technical standards, in order to have real meaning and effects.322 Following previous discussions, given that ML blurs the line between research and development, a robust system of T&E/V&V is necessary, both at national and at Alliance level.323 Working together on these standards is crucial to ensure that Allies can plug together their capabilities and that the same parameters are adopted, both for combat effectiveness and for economic efficiency.

Approach to standards. AI does raise new challenges, but this does not mean that all new challenges require new solutions. Some standards, for instance, can be imported horizontally from nearby fields, like that of cyber security. This issue highlights the importance of the approach to standards, which NATO Allies may want to discuss: should new standards be pursued when it comes to AI, or should countries agree to use existing ones? Should they opt for stable standards, or try to update them regularly? These are important questions. For instance, the U.S. National Institute for Standards and Technology provides a list of features that the US should pursue for standardization – e.g., innovation-oriented, applicable across sectors and applications, human-centred.324 The Atlantic Alliance would benefit from a similar discussion as well as, eventually, trying to coordinate each Ally’s preferences, position and approaches towards standard multinational standard-setting forums, like Standard Development Organizations.

Standards and effectiveness. One of the main challenges of the interaction between algorithms and BD is their brittleness.325 Algorithms can be (easily) fooled. In the civilian economy, this may lead to controversial or even unacceptable outcomes, such as discrimination or bias.326 For instance, HR algorithms may discard some candidates because historical underrepresentation of their sex or ethnicity disadvantages them in the data on which the recommender algorithm is trained. In the military domain, this may lead to errors, like mistaking a military target for a civilian facility or the other way around, and overall combat ineffectiveness, or even defeat. The use of generative adversarial networks which intentionally exploit these vulnerabilities to undermine the opponent’s capabilities makes matters worse.327 To address these problems, AI and related technologies must comply with a set of principles that standards can translate and consolidate, including safety and reliability as well as accepted degrees of accuracy. Non-technical standards can also play an important role in defining procedures, processes and approaches in developing and fielding those systems, including about issues related to human control.328 However, standards should be also complemented by tools to enable the development of effective, reliable, robust and trustworthy AI technologies, in areas such as accountability and auditing, annotations and documentation, benchmarks, metrics, AI testbeds, methodologies and datasets in standardized formats.

### 2AC---AT: Process CP

#### Consultation fails---needs to be faster

Simona R. Soare 21, was a Senior Associate Analyst at EUISS from 2019 to end May 2021. Her research focused on United States security policy, transatlantic security and EU-NATO relations. Prior to joining EUISS, Simona served as advisor to the Vice-President of the European Parliament (2015-2019) and as an analyst with the Romanian Ministry of Defence, working on transatlantic and European security. She has also been a research associate with the Institut d’Études Européennes (IEE) at Université Saint Louis-Bruxelles. Simona holds a PhD in Political Science from the National School for Political and Administrative Studies in Bucharest where she lectured on international security (2008-2015). She is the recipient of a U.S. Department of State fellowship on U.S. Grand Strategy and has published extensively on American and transatlantic security. "Innovation as Adaptation: NATO and Emerging Technologies" June 11. <https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies> //pipk

There is great convergence and commonality among the recommendations of the Advisory Group on Emerging and Disruptive Technologies and the NATO 2030 Reflection Group. Both call for the establishment of transatlantic digital consultations and dedicated structures, including a NATO Advanced Technology Projects Agency and funding instruments such as a NATO Investment Bank. Building on these recommendations, as well as on NATO-private sector dialogues, in February Secretary-General Jens Stoltenberg proposed the establishment of a NATO Defense Innovation Initiative “to promote interoperability and serve as a catalyst for transatlantic cooperation on defense innovation.”18 After consultations and meeting political roadblocks, the allies decided to establish the Defense Innovation Accelerator instead as a more flexible, opt-in, and off-budget instrument.

The NATO 2030 agenda thus incorporates innovation and EDTs under the broader mantra of an “ambitious program for the continued adaptation of the alliance.”19 However, NATO’s history of adaptation also underlines important limitations and challenges.20 These include challenges in speed of adoption, spending levels, technological compartmentalization, fragmented and incomplete information and skills, stovepiped innovation practices, fragmented national innovation initiatives, lagging NATO-EU cooperation, allied technology and digitalization gaps, and a general underuse of NATO instruments to pursue collaborative defense innovation in EDTs.21 Faced with the prospect of long-term competition with technically capable China and Russia, NATO’s history of incremental adaptation may be too slow, prescriptive, or inflexible for successful innovation.

In this context, speed is crucial. NATO’s efforts must break the cycle of incremental adaptation and lay the foundation for a more dynamic and strategic innovation process. Defense innovation in EDTs cannot be tied to NATO’s decade-long policy and adaptation cycles because this may not be enough to innovate at the pace of relevance. The new Defense Innovation Accelerator and AI Strategy should become long-term, staple tools for the alliance to build a culture of rapid experimentation and innovation uptake and a resilient innovation ecosystem within it.

Innovation as Adaptation

In the context of the rapid pace of progress in several technologies driven by the private sector and market forces, NATO’s approach to innovation and EDTs stands out in comparison to previous adaptation efforts in the 1990s and 2000s. The ongoing reflection in the Emerging and Disruptive Technologies Roadmap and the NATO 2030 process is perhaps one of the most systematic efforts to develop a strategic and coordinated approach to several technology priority areas, backed simultaneously by institutional change and procedural innovation. Today’s iteration of defense innovation seems an order of magnitude and speed above what the alliance has experienced before. It builds on substantial changes in NATO processes, structures, authorities, and skills to reward risk taking and experimentation. NATO’s innovation efforts also go beyond the traditional focus on technical and operational standardization, and they include a prominent ethical and normative dimension. As the NATO secretary-general recently underlined, allies “should also look into how NATO can be the platform to address ethical aspects of these technologies,” including by developing “guideline standards.”22

#### Process CP is bad---can’t solve, risks delays, undermines allies commitments---streamlining is key

R. Clarke Cooper 21, nonresident senior fellow at the Atlantic Council, former assistant secretary at the US Department of State, a former senior intelligence officer for the US Joint Special Operations Command. December 23. "A multipolar world requires more adaptive US security thinking" <https://www.atlanticcouncil.org/blogs/new-atlanticist/a-multipolar-world-requires-more-adaptive-us-security-thinking/> //pipk

While the scale and volume of military interventions by China, Russia, and Iran are reportedly lower now than at the height of Cold War, the increasing risks of disruptive actions by these state actors and their proxies in a multipolar world require deterrence featuring robust technological solutions, which can only emerge from smart, adaptive policy.

The United States and its security partners are awaiting the Biden administration’s Global Posture Review, along with the potential expansion of security cooperation procedures, expanded congressional reviews, and a revision of the Conventional Arms Transfer (CAT) Policy—which would further protract an already lengthy arms-sale process. Meanwhile, dictatorial adversaries of democracy and freedom in Beijing, Moscow, and Tehran are aggressively seeking opportunities for disruption wherever Washington might expand or reduce security cooperation, or simply withdraw its presence. Ready access to low-cost, but effective, commercial technologies render that threat even more potent.

For the United States to remain a leader in this new multipolar world and more effectively plan its global posture, it must snap out of a Cold War-style mindset, cut down on bureaucracy, and refrain from expanding processes that hamstring security cooperation.

The Trump administration made some notable advances to promote innovation and protect US technological advantage through its 2017 National Security Strategy; 2020 National Strategy for Critical and Emerging Technologies, designed to actively promote innovation; and its commitment to revise the US export policy for Unmanned Aerial Systems (UAS). These policies were a good start, but not enough. Now President Joe Biden has an opportunity to bring them to fruition.

To understand the rapid emergence of UAS threats, look no further than the growth of Iran’s military drone program in recent years, which also extends to Iran-backed groups across various regional conflicts. This includes Houthi rebels in Yemen using drones against Saudi Arabia, Hamas deploying them against Israel in the Gaza Strip, and Iraq-based Shia militia using them to attack US troops—likely including the recent drone attack on Al Tanf, a remote US outpost on the Syrian-Jordanian border. Iran’s increasing use of this technology, specifically “suicide” or “kamikaze” drones that fly into their targets and explode, requires integrated air defenses and Counter-Unmanned Aircraft Systems (C-UAS) technology. Regional US partners in the Middle East, which have increasing requirements to deter Iranian aggression, will seek every opportunity to acquire it from the US government.

The US security establishment has long acknowledged that adversaries like China and Iran are pursuing commercial, off-the-shelf technologies that can threaten US personnel, penetrate allies’ and partners’ air defenses, and generally challenge regional stability. But the US approach still has room for improvement.

As part of its new CAT policy, the Biden administration is considering expanding bureaucratic processes for arms sales to better safeguard US interests—but this inadvertently chips away at the prime placement of American aerospace and defense industries in the global marketplace. Extending the processes for military arms sales and transfers risks ceding the security cooperation space to US adversaries. The United States has a unique role in the world, and its national-security interests—including its defense industrial base—shouldn’t be compromised (certainly not by the government) in pursuit of a “level playing field,” as recently advocated by Assistant Secretary of State for Political-Military Affairs Jessica Lewis. For the US government to suggest putting US industry on par with competitors is counterintuitive; it is a national- and economic- security imperative for the government to bolster US industry to excel with every possible advantage.

US security cooperation historically encompasses facilitating arms sales, staging military training and exercises, developing interoperability among allies and partners, and bolstering the sovereign defense capabilities of security partners. All these efforts need to continue at a deliberate pace—but in a post-Cold War world, the United States no longer has a monopoly on arms sales with an overt technological advantage in all areas.

In recent years, intelligence, surveillance, and reconnaissance capabilities became the focus of Chinese UAS production, and as then Chairman of the Joints Chiefs of Staff Joe Dunford noted in 2018, “Whoever has the competitive advantage in artificial intelligence and can field systems informed by artificial intelligence, could very well have an overall competitive advantage.” Many of us in the national-security enterprise at the time were also concerned with how AI innovation would shape the development of drones and integrated air-defense systems. With that technological competition heating up, allies and partners matter more than ever.

To remain the “partner of choice” for its allies and partners, the United States needs to work closer with them in collaborative partnerships, such as the trilateral AUKUS defense pact among the United States, Australia, and the United Kingdom. It can also develop other proactive collaborative schemes in emerging technologies to enhance shared capabilities and interoperability, help security partners successfully meet updated UAS export policy, and aggressively advocate for and develop integrated air-defense capabilities.

For the sake of American interests, the US government must carefully foster its partnerships and spark a level of defense innovation to keep the United States and its partners truly secure.

### 2AC---AT: Security Cooperation PIC

#### Security coop cred good---signals to allies

R. Clarke Cooper 21, Nonresident Senior Fellow, Atlantic Council. Former U.S. Assistant Secretary of State for Political-Military Affairs. Former U.S. Alternate Representative to the United Nations Security Council. Rafik Hariri Center & Middle East programs Scowcroft Middle East Security Initiative. September 3. "American security cooperation needs an ‘integrity check’" <https://www.atlanticcouncil.org/blogs/new-atlanticist/american-security-cooperation-needs-an-integrity-check/> //pipk

Since World War II, US presidents have understood the tremendous value of security cooperation, prompting them to invest in alliances and partnerships. These are, after all, significant components of US national security, and as President Joe Biden recently noted, “America’s alliances are our greatest asset.”

Yet successful security cooperation—which includes arms transfers, training, security assistance, treaties, or agreements—is built around two key principles: trust and integrity of commitment, both of which are at risk today thanks to the haphazard US withdrawal from Afghanistan.

In the US military, the term “integrity check” refers to a concern about an individual’s or unit’s capability or trustworthiness. Following the debacle in Kabul, the United States and its global security cooperation posture is in dire need of one.

Just look at the anger expressed by stalwart NATO allies such as the United Kingdom, which in the aftermath of 9/11 unquestionably joined in to invoke the Washington Treaty’s Article 5 for collective self-defense (the first time the Alliance ever did so). That NATO launched its first operations outside the Euro-Atlantic area and began a far-reaching transformation of capabilities signaled its trust in the United States’ reliability when it came to security cooperation.

Now, treaty allies and partner nations are reassessing their bilateral security relationships with the United States. It’s not just the NATO states caught off-guard by the haphazard departure from Afghanistan that will think twice before embarking upon future military campaigns with the United States. Resolute defense partners in the Middle East and the Indo-Pacific—including Saudi Arabia, Jordan, Qatar, Japan, South Korea, and Taiwan—likely also need overt reassurance, such as a clear national-security strategy and declared recommitments.

Additionally, these partners are increasingly feeling the need to proactively raise their own defense capabilities by boosting their budgets or coordinating with allies to ensure regional security along with the United States.

Besides stress-testing the integrity of American security cooperation, the Afghanistan withdrawal also highlights the necessity of staying the course on long-term investment in mutually beneficial security partnerships with countries with which the United States has shared interests—or shared threats. Well before the fall of Afghanistan, foreign partners were already questioning the reliability of the United States at a time when the debate in Washington about our global posture was becoming increasingly politicized.

The case for partnering with the United States needs to be clearly articulated through the presence, performance, and processes of American security cooperation. The quality of US aerospace and defense equipment, the commitment to build capabilities, and the reassurance that comes from partnering with the US military must include further transparency, accountability, and predictability of policies.

If not, American allies and partners will be hesitant to collaborate with us on future shared security requirements—or simply seek cooperation elsewhere.

We owe it to our fellow Americans, as well as to allies and partners, to be candid about the costs of security and what it takes to support our shared values of the rule of law, civil society, and human rights. As we await the outcome of the Global Posture Review, or a revised Conventional Arms Transfer Policy, anti-democratic adversaries in Beijing and Moscow are aggressively exploiting each disruption associated with the Taliban takeover in Kabul.

If alliances are indeed our “greatest asset”—whether in the Middle East, Indo-Pacific, Africa, or Europe—it is crucial for US officials to actively affirm their values through clear recommitments and presence in security cooperation, such as the recent pledges made to Israeli Prime Minister Naftali Bennett and Ukrainian President Volodymyr Zelenskyy.

We would be naïve to believe that countries around the world have no choice but to partner with the United States. Washington must be deliberate in its efforts to prove why choosing the United States as a security partner remains the best option.

## AT: Disads

### 2AC---Link Uniqueness---NATO AI

#### All the disads are thumped

Vivienne Machi 21, reporter based in Stuttgart, Germany, contributing to Defense News' European coverage. She previously reported for National Defense Magazine, Defense Daily, Via Satellite, Foreign Policy and the Dayton Daily News. She was named the Defence Media Awards' best young defense journalist in 2020. "NATO ups the ante on disruptive tech, artificial intelligence" November 3. <https://www.defensenews.com/digital-show-dailies/feindef/2021/11/03/nato-ups-the-ante-on-disruptive-tech-artificial-intelligence/> //pipk

Artificial intelligence

Meanwhile, the allies also agreed on NATO’s first-ever artificial intelligence strategy, which has been in the works since early 2021. “It will set standards for responsible use of artificial intelligence, in accordance with international law, outline how we will accelerate the adoption of artificial intelligence in what we do, set out how we will protect this technology, and address the threats posed by the use of artificial intelligence by adversaries,” Stoltenberg said.

NATO released a summary of the strategy on Oct. 22, and it includes four sections: Principles of responsible use of artificial intelligence in defense; ensuring the safe and responsible use of allied AI; minimizing interference in allied AI; and standards.

It also lays out the six principles of AI use that member-nations should follow. They include: lawfulness; responsibility and accountability; explainability and traceability; reliability; governability; and bias mitigation.

The nascent DIANA outfit will host specialized AI test centers that will help NATO ensure standards are being kept as member-nations develop new platforms and systems and encourage interoperability, van Weel noted. That way, NATO creates “a common ecosystem where all allies have access to the same levels of AI,” he said.

NATO will also form a data and artificial intelligence review board with representatives from all member-nations, to ensure the “operationalization” of the AI strategy, he added. “The principles are all great, but they only mean something if we’re able to actually translate that into how the technology is being developed, and then used.”

### 2AC---AT: Military AI Bad DA

#### AI integration into the military is inevitable globally

Erik Lin-Greenberg 20, postdoctoral fellow at the University of Pennsylvania’s Perry World House. Texas National Security Review, Vol 3, Iss 2. Spring. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making" <https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/> //pipk

Broadly defined, AI is the ability of computers and machines to perform tasks that traditionally require human intelligence.22 AI has been applied to control self-driving cars and swarms of unmanned aircraft, to assist physicians in making medical diagnoses, and at the more quotidian level, to screen spam emails and act as virtual personal assistants.23 Underlying AI technologies are a variety of approaches including mathematical optimization, statistical methods, and artificial neural networks — computer systems that attempt to perform specific tasks in a similar way to the human brain.24 Regardless of approach, AI typically uses large amounts of data to train and feed algorithms to accomplish tasks and processes that are normally associated with human cognition. Most current AI is considered to be “narrow,” designed to achieve a specific task — like identifying objects in images. Researchers, however, are working to develop artificial general intelligence that can accomplish any task the human brain can.25

Narrow AI technology has increasingly been applied in the national security domain. Although much policy and scholarly writing focuses on lethal autonomous weapon systems — “killer robots” that can identify and engage targets without human intervention — AI is far more commonly employed in a range of more mundane military and national security tasks.26 In some cases, AI is part of analytical processes, like the use of machine learning to classify targets in satellite imagery.27 In other instances, it is part of the software used to operate physical systems, like autonomous planes or ships.28 In both cases, AI is not a military capability in itself, but an enabler that can enhance the efficiency of military tasks and systems.29

Many regional and global military powers have already fielded AI-enabled military systems.30 Israel and Russia, for instance, have reportedly tested self-driving tanks and armored vehicles capable of identifying targets without human direction.31 The United States is making headway on Project Maven, the Defense Department’s effort to use machine learning — an application of AI — to streamline the analysis of video gathered by drones.32 Similarly, Japan’s Self-Defense Force announced that it will equip its P-1 maritime patrol aircraft with AI technology that will more effectively identify vessels and other potential targets.33 States have also begun incorporating AI into autonomous systems that can navigate without direction by human operators, often in swarms intended to overwhelm an enemy’s defenses. In 2017, for instance, the U.S. Naval Postgraduate School and the Defense Advanced Research Projects Agency hosted a large-scale experiment where swarms of autonomous drones flew simulated combat missions against each other.34

The development of these systems should not come as a surprise. Military and political decision-makers seek to enhance the efficiency and accuracy of their state’s military and to reduce risk and costs during operations. AI can help accomplish these objectives. In many contexts, AI can make assessments and judgements with greater speed and accuracy than humans, and with less manpower. For example, AI can help quickly dig through vast quantities of imagery and video data to pinpoint objects of interest, like military vehicles, with little human involvement.35 In contrast, geospatial intelligence exploitation that is not assisted by AI is a time-intensive and manpower-intensive process.36 AI can also be used to operate autonomous weapon systems that allow states to launch military operations without putting friendly personnel in harm’s way. These systems can decrease the risk of friendly casualties and reduce the political barriers to launching military operations.37 The efficiency-enhancing and risk-reducing characteristics of AI-enabled systems will likely appeal to casualty-averse and cost-conscious leaders. Indeed, AI technologies might allow these leaders to launch operations not previously possible because of efficiency concerns or high degrees of risk to friendly forces.

### 2AC---AT: AI Cooperation Bad DA

#### International AI cooperation high now---US cred high---other things prevent cooperation

Andrew Imbrie et al 20, Andrew Imbrie Ryan Fedasiuk Catherine Aiken Tarun Chhabra Husanjot Chahal. Center for Security and Emerging Technology (CSET) at Georgetown’s Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. February. "Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI" //pipk

All surveyed officials indicated that they engage with international partners on AI-related issues. Bilateral efforts were the most cited avenue of international collaboration on AI, in four cases (EU, Australia, Czech Republic, and Italy) involving the United States. Multilateral fora were another common and increasingly relevant avenue for collaboration. The Organization for Economic Cooperation and Development (OECD) was the most cited multilateral forum, while multiple officials indicated engagement through the EU, Group of Seven (G7), Group of Twenty, or the newly created Global Partnership on AI (GPAI). Current international efforts focus on developing shared ethical standards, in part following the lead of the OECD and EU on defining AI standards. Other officials noted collaboration around workforce challenges, data policies, climate change, and lethal autonomous weapons systems (LAWS).

Partners’ active engagement and interest in international collaboration around AI is matched with positive perceptions of the United States’ role as an AI partner. Eighty percent of officials said their country considers the United States to be a reliable partner on AI issues. The remaining three officials, representing the EU, Germany, and France, suggested that while they consider the United States a like-minded ally and continue to value U.S. partnership, recent exchanges have been less fruitful and current approaches raise general concerns regarding U.S. reliability as an AI partner. Officials also rated the United States highly in terms of commitment to responsible use of AI with an average rating similar to the average rating of their own countries, or institutions, in the case of the EU, and a significantly higher rating than they assigned to China’s commitment to responsible AI (7.3, 7.9, and 3.8 out of 10, respectively).

In citing obstacles to collaboration with the United States, officials were split between placing blame on the United States and on their own country. Multiple officials noted threats to industry and industrial competition, trade issues, different domestic priorities, or a lack of agreed upon strategy or common structures as obstacles to collaboration. Others specified that the U.S. desire to “win” relative to China, lack of data privacy protection, or unwillingness to engage inhibited collaboration. They also noted a lack of confidence in current U.S. goals or appropriate U.S. points of contact. Obstacles stemming from their own government included a lack of regulatory framework or set policies, alternative political priorities, a preference for multilateral fora, or insufficient resources.

The survey results indicate that there is space for the United States to engage with international partners and, despite some specific but not insurmountable points of difference, a high degree of alignment on AI interests and priorities.

### 2AC---AT: US Military AI Bad DA

#### US has already integrated AI into military assets

Erik Lin-Greenberg 20, postdoctoral fellow at the University of Pennsylvania’s Perry World House. Texas National Security Review, Vol 3, Iss 2. Spring. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making" <https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/> //pipk

The U.S. military has already started to develop this type of capability. As part of a series of exercises, the Defense Department demonstrated a command-and-control network that uses AI to automatically detect enemy activity and pass targeting information between multiple intelligence and military assets. During one of these exercises, a space asset detected a simulated enemy ship, but was unable to identify it. The network automatically cued an intelligence, surveillance, and reconnaissance platform to collect additional information on the adversary vessel, which it then sent to a command-and-control asset. The command-and-control platform used AI to select the best platform available to strike the enemy ship and passed targeting data to the nearby U.S. naval destroyer that would engage the adversary vessel. AI significantly shortened the targeting process relative to efforts without AI technology. When describing the AI-enabled network in November 2019, U.S. Air Force Chief of Staff Gen. David Goldfein announced, “This is no longer PowerPoint. It’s real.”90

#### US integrating AI into military operations now

Matej Tonin 19, current Slovenian Minister of Defense, was an active member of the NATO PA from 2012 to 2020. He served as rapporteur and Chairperson of the Assembly's Sub-Committee on Technology Trends and Security and as Deputy Head of the Slovenian delegation to the NATO PA. "ARTIFICIAL INTELLIGENCE: IMPLICATIONS FOR NATO’S ARMED FORCES" Report from the Sub-Committee on Technology Trends and Security. October 13. <https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf> //pipk

A. THE UNITED STATES 45. As the global leader in AI, the United States has actively sought to integrate AI into its military capabilities. Defence-related AI continues to be a big part of the efforts started under the Obama administration’s Third Offset Strategy, aimed at the preservation of the US military advantage. In 2018, the US Department of Defense (DoD) published its own AI strategy, which will certainly be reinforced by the national American AI Initiative launched by the Trump administration in February 2019.

46. The DoD continues to invest significant resources in AI-related programmes and initiatives. A 2017 report estimated that, between 2013 and 2017, approximately USD 1.76 billion were devoted to three categories of relevant DoD spending (learning and intelligence; advanced computing; and AI systems) (Govini, 2017). In 2018, the Defense Advanced Research Projects Agency (DARPA) announced an additional USD 2 billion between 2018 and 2023. In 2016, the DoD created the Defense Innovation Unit (DIU) to facilitate the integration of commercial technology into the military. As the STC learned when meeting with DIU officials in October 2018, AI is a key area of the DIU’s activities. In 2018, the DoD also established a Joint Artificial Intelligence Center (JAIC), whose Chief Architect laid out JAIC’s aims during the October 2018 STC visit. JAIC has been allocated a budget of USD 1.75 billion for six years to oversee and coordinate DoD AI efforts.

47. The US military is engaged in numerous AI-related projects and programmes. A few examples illustrate the breadth of these activities: - DARPA’s Target Recognition and Adaptation in Contested Environments (TRACE) programme has delivered promising technologies, such as an automatic target-recognition system to assist pilots. - The US Air Force is currently developing such a system, called Multi-Domain Command and Control, to better integrate the extensive data collected from its wide range of sources. - Project Maven is an important information, surveillance and reconnaissance (ISR) programme, developed together with US tech giants such as Google, Microsoft, and Amazon. It helps human analysts, through computer-vision technologies, to process up to two to three times as much data in the same time period (CRS, 2018). The system is already in use in counter-Daesh operations. - The US Army is testing Uptake’s Asset Performance Management application to employ predictive maintenance in its M-2 Bradley infantry fighting vehicles. The STC delegation heard more about this topic from Uptake’s leadership during the 2018 Silicon Valley visit. - The Army is working on optionally manned Next-Generation Combat Vehicles. - The Air Force Research Lab has initiated the Skyborg programme that seeks to train US Air Force pilots through an AI system, possibly hosted on an unmanned aircraft (Insinna, 2018). - DARPA held a Cyber Grand Challenge pitting autonomous machines against one another. Each of these machines was designed with vulnerabilities, and contestants had to create AI algorithms capable of identifying and fixing these weaknesses while attacking their opponents (Hoadley and Lucas, 2018). - The US Army is developing a tool called Macroscope which uses data produced by social networks to better understand social environments.

### 2AC---AT: Europe Military AI Bad DA

#### Europe investing in military AI now

Matej Tonin 19, current Slovenian Minister of Defense, was an active member of the NATO PA from 2012 to 2020. He served as rapporteur and Chairperson of the Assembly's Sub-Committee on Technology Trends and Security and as Deputy Head of the Slovenian delegation to the NATO PA. "ARTIFICIAL INTELLIGENCE: IMPLICATIONS FOR NATO’S ARMED FORCES" Report from the Sub-Committee on Technology Trends and Security. October 13. <https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf> //pipk

B. EUROPE 48. European states and the EU have increasingly recognised the growing importance of AI technologies and applications. Indeed, all EU member states and the European Commission have now adopted AI strategies. Many countries and the EU itself have substantially increased AI funding and set up organisational structures and entities to deal with the opportunities and challenges of AI. However, Europe is confronting a number of structural challenges. In terms of hardware, European actors still rely heavily on US chipmakers. Moreover, it faces intense competition from the United States where salaries are more attractive to European researchers. Europe is also comparatively less successful at translating research into commercial products. Finally, Europe’s comparatively stricter data security rules, which most Europeans value very highly, restrains its access to data pools (Franke, 2019). To deal with privacy and other ethical concerns, an EU HighLevel Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence in April 2019.

49. As the EU builds up its defence initiatives, notably the European Defence Fund and the Permanent Structured Cooperation, defence-related AI R&D could certainly play an important role. For now, however, most efforts are designed and implemented at the national or bilateral levels, with the United Kingdom and France taking the leading role within Europe.

### 2AC---AT: China AI Bad DA

#### China integrating military AI now

Matej Tonin 19, current Slovenian Minister of Defense, was an active member of the NATO PA from 2012 to 2020. He served as rapporteur and Chairperson of the Assembly's Sub-Committee on Technology Trends and Security and as Deputy Head of the Slovenian delegation to the NATO PA. "ARTIFICIAL INTELLIGENCE: IMPLICATIONS FOR NATO’S ARMED FORCES" Report from the Sub-Committee on Technology Trends and Security. October 13. <https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf>

C. CHINA 53. AI has become a top priority for Chinese leaders, both for commercial and military applications. As articulated in the 2017 New Generation AI Development Plan, China is aiming to become the global AI leader and develop a domestic AI market worth USD 150 billion by 2030. Already today, the government and industry have begun to believe that China has “largely closed the gap with the United States in both AI R&D and commercial AI products” (Allen, 2019). However, significant gaps remain in a number of areas, for example AI talent, technical standards, software frameworks and platforms, and semiconductors (Allen, 2019). China-based companies already play a significant role in the global development of AI technologies. Not only is China investing at home, but the country has also been investing abroad, which draws increased scrutiny by Allies.

54. As two Committee speakers outlined at the 2019 Spring Session, the entanglement of the private sector with public institutions, such as the party-state and the armed forces, significantly facilitates the incorporation of AI technologies into the defence sector, since top-down coordination clearly guides companies’ development priorities. The emphasis put by President Xi Jinping on “military-civil fusion” is likely to sustain this trend (Sheppard et al., 2018). Moreover, China has been an early adopter of AI technologies for domestic surveillance applications. This lowers the barriers to adoption of AI-enabled systems by the military (Allen, 2019). Lower privacy standards compared to North America and Europe, combined with the sheer numerical advantage of the private data collected, provide a key advantage for developing new AI algorithms, too.

55. Analysts believe China’s efforts to integrate AI into its military spectrum are informed by AI developments in other countries, notably the United States. China believes in a “military revolution of intelligentisation” (De Spiegeleire, Maas, and Sweijs, 2017). The Chinese government views the disruptive potential of AI as an opportunity to “leapfrog” the United States by investing heavily in novel disruptive systems, rather than only sustaining legacy systems (Allen, 2019). For example, Beijing has focused on the potential of AI for enhanced battlefield decision-making, cyber capabilities, cruise missiles, and autonomous vehicles in all military domains – all technologies which could present great difficulties for the United States in a conflict.

### 2AC---AT: Russia AI Bad DA

#### Russia investing military AI now

Matej Tonin 19, current Slovenian Minister of Defense, was an active member of the NATO PA from 2012 to 2020. He served as rapporteur and Chairperson of the Assembly's Sub-Committee on Technology Trends and Security and as Deputy Head of the Slovenian delegation to the NATO PA. "ARTIFICIAL INTELLIGENCE: IMPLICATIONS FOR NATO’S ARMED FORCES" Report from the Sub-Committee on Technology Trends and Security. October 13. <https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf> //pipk

D. RUSSIA 56. President Vladimir Putin has declared that “AI is the future […]. Whoever becomes the leader in this sphere will become the ruler of the world”. Although Russia still lags behind the United States and China, it has demonstrated its commitment to catching up with its competitors – at least in certain areas. Nevertheless, while Chinese and US companies spend billions of US dollars in AI, the Russian private sector only invested an estimated RUB 700 million annually (less than USD 11 million at the time of writing) (Horowitz et al., 2018). New reports indicate, however, that the Russian Direct Investment Fund has recently raised USD 2 billion from foreign investors to support the domestic AI sector (bne IntelliNews, 2019).

57. The Ministry of Defence, along with elements of the defence industry, has assumed a leading role on AI. For one, the Russian Military Industrial Committee seeks to make 30% of its military equipment remotely controllable by 2025 (Allen and Chan, 2017). As part of this push, the Russian government created the Advanced Research Foundation, Russia’s response to DARPA, whose annual budget stands at approximately RUB 4 billion (about USD 62 million at the time of writing). The agency has so far focused on technologies imitating human thinking, data analysis, and assimilation of new knowledge. It has also singled out four main lines of effort that AI developments should follow: image recognition; speech recognition; control of autonomous military systems; and life-cycle support for weapon systems (Bendett, 2018). Russia’s AI national strategy is expected to be published in June 2019. In May 2019, President Putin outlined some of the strategy’s priorities: training programmes, public-private partnerships, new legislation, and building on the country’s strengths in science, technology, engineering and mathematics (Bendett, 2019). He and several ministers also hinted that up to USD 1.4 billion could be invested into domestic AI efforts to develop “technological sovereignty” in AI (Bendett, 2019).

58. Russian industries are integrating AI into weapons systems, especially robotic autonomous systems (Hoadley and Lucas, 2018). The Kalashnikov Group has reportedly developed an AI-controlled ground vehicle with neural network AI technology (IISS, 2018). The radio-electronic company KRET has reportedly been working on “unmanned systems with swarming and independent decision-making capabilities” (IISS, 2018). Moreover, the Russian Air Force has announced the development of AI-guided missiles. Analysts also argue that Russia’s robust development of civilian technologies on image and speech recognition will likely be incorporated into Russian information operations (Bendett, 2018). It must be noted that Russia’s ambitious AI plans may be hindered by structural challenges such as the weakness of Russia’s technology industry and falling defence budgets (Hoadley and Lucas, 2018).

### 2AC---AT: EU Tradeoff DA

#### No EU tradeoff

EU Institute for Security Studies 19, The European Union Institute for Security Studies (EUISS) is the Union’s agency dealing with the analysis of foreign, security and defence policy issues. Its core mission is to assist the EU and its member states in the implementation of the Common Foreign and Security Policy (CFSP), including the Common Security and Defence Policy (CSDP) as well as other external action of the Union. "The EU Nato and Artificial Intelligence" November 14. <https://www.iss.europa.eu/sites/default/files/EUISSFiles/EU%20NATO%20AI%20-%20Report.pdf> //pipk

However, the conference also addressed specific challenges to cooperation. It was pointed out that the two organisations occasionally held diverging perspectives on particular issues, such as Lethal Autonomous Weapon Systems (LAWS) or the appropriate balance between laissez-faire and dirigiste approaches to defence industrial and technological matters. The fact that not every EU member state had published their positions on AI yet, while the US AI military strategy does not even mention NATO, did little to bridge these divergent viewpoints. It was also highlighted that despite any possible need for cooperation on AI, the respective mandates and autonomy of each organisation should be respected.

NEXT STEPS FOR EU-NATO COOPERATION A shared view at the event was that moving EU-NATO cooperation forward was essential. As in the cyber domain, the two organisations could play complementary roles, drawing on their respective strengths and instruments, with the EU leading in dual-use and NATO in military standards. The importance of shared values and outlooks was also highlighted on several occasions. The two organisations held similar perspectives on fundamental issues, including the unknown qualities of AI in defence, the need for technological partnership between democracies, an AI arms control regime and strong links between government and industry. In addition, cooperation required a shared understanding of AI. Creating a common vocabulary was key in this respect, an area that the European Defence Agency (EDA) was already working. It was also noted that inter-institutional cooperation would not be fully effective until each organisation developed an internally coherent outlook, with clearly defined goals, threat perceptions and a goal-driven approach to AI.

#### NATO AI testing and standards solves integration with the EU

EU Institute for Security Studies 19, The European Union Institute for Security Studies (EUISS) is the Union’s agency dealing with the analysis of foreign, security and defence policy issues. Its core mission is to assist the EU and its member states in the implementation of the Common Foreign and Security Policy (CFSP), including the Common Security and Defence Policy (CSDP) as well as other external action of the Union. "The EU Nato and Artificial Intelligence" November 14. <https://www.iss.europa.eu/sites/default/files/EUISSFiles/EU%20NATO%20AI%20-%20Report.pdf> //pipk

On this basis, a number of specific areas for increased EU-NATO cooperation were discussed during the discussion. It was proposed that further steps were taken to implement the Joint Declarations, including possibly by establishing an ‘AI Centre of Excellence’. Another proposal concerned adding an AI research dimension to the Declarations, although a different view contended that AI would nonetheless automatically and incrementally feature in EU-NATO cooperation given its crosscutting nature. The need for a common EU-NATO data-management and data-sharing framework was also proposed, in light of the importance of data pools for the performance of AI algorithms. Although much remained to be done in that area, data labelling was identified as a good starting point.

Another point raised on several occasions was the importance of interoperability. Here, it was argued, AI had the potential to either increase or decrease existing gaps. Militaries could mitigate AI interoperability gaps through exercises and common training, such as through the Cyber Education Platform, or by developing niche capabilities, especially by utilising EU initiatives such as Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF). Some participants argued that divergences were nevertheless inevitable and that, consequently, countries with low or no AI capabilities should be able to trust the technologies of those with more advanced technologies. This, in turn, required a common framework for certification and evaluation procedures, as well as standardised interfaces and modular system architectures that would combine closed/‘national’ and open/‘shared’ components.

### 2AC---AT: Relations Tradeoff DA

#### Security cooperation doesn’t trade off with other countries

Michael J. Mazarr et al 22, senior political scientist at the RAND Corporation. "Security Cooperation in a Strategic Competition" Research Report. <http://www.rand.org/t/RRA650-1> //pipk

There is not necessarily a competition in security cooperation per se, and security cooperation activities among major rivals are not necessarily mutually exclusive. Our analysis in this study suggests that U.S. security cooperation activities seldom directly compete with those of U.S. rivals, other than through those activities’ contribution to overall influence. Many of the case studies reveal that the United States engages in significant levels and types of security cooperation with countries that are pursuing similar activities with Russia, China, or both. There are few cases in which Russian or Chinese security cooperation prevented or obstructed parallel U.S. activities (although arms sales could be seen as an exception). Security cooperation is best viewed as one piece of a much larger competition for influence; security cooperation activities themselves are usually not zero-sum.

### 2AC---AT: Brain Drain

#### P3s solve

Andrew Imbrie et al 20, Andrew Imbrie Ryan Fedasiuk Catherine Aiken Tarun Chhabra Husanjot Chahal. Center for Security and Emerging Technology (CSET) at Georgetown’s Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. February. "Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI" //pipk

The global competition for AI talent is nominally zero-sum, but talent development efforts such as education and training could expand it. The United States should cultivate international networks of researchers through exchange programs. One potential model is the U.S. Telecommunication Training Institute, which brings officials from developing countries to the United States for tuition-free training in information and communications technologies. Such programs would enable U.S. and allied policymakers to identify comparative advantages in AI, share best practices, and promote linkages and the free flow of ideas between government, industry, and academia.

The right approach would facilitate the exchange of knowledge and best practices among allied and partner countries. The NSF, for example, has awarded grants to researchers who seek to promote international collaboration and benefit from the expertise and specialized skill sets of international partners.84 Additional programs, joint scholarships, and conference support could synchronize efforts to grow the pool of AI talent. Survey results suggest that partners already engage in various efforts to leverage international ties to encourage STEM education, provide AI-relevant fellowships, and offer AI-specific advanced and technical degrees.

Exchanges and fellowship programs could also mitigate zero-sum dynamics, such that when a country “loses” AI talent to an ally or partner, it nevertheless gains from the capabilities and networks of which its researchers are a part. To further this effort, the U.S. government should commit resources to hosting and convening workshops among AI researchers, fostering international networks of AI researchers, and deepening partnerships with existing networks, such as the Confederation of Laboratories for Artificial Intelligence Research in Europe (CLAIRE). The United States and its allies should coordinate with the private sector from the outset on job placement and training programs, including hosting recruiting sessions that bring together representatives from government, industry, and academia. Surveyed officials from the United Kingdom, Chile, Colombia, and Japan noted ongoing public-private partnerships to foster AI talent, including providing subsidized training courses, promoting women in STEM, and talent development programs.

#### Aff solves AI shortages---cooperation through NATO leads to coordination that solves

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

Building on the previous discussion of AI as a GPT, it appears that the challenge for NATO is subtle, multifaceted and significant. First, in an age of accelerating technological change and growing domain applicability, catching up with industry leaders and innovators becomes more and more difficult for those that lag behind.73 This means that waiting is not a solution – even though acting prematurely, in a realm of great uncertainty, is inherently difficult and risky.74 Second, governments cannot expect that individuals, firms and organizations will be able to embrace and successfully exploit the new wave of technological transformation alone, without advice, support, direction, vision or investments in infrastructure. Third, while some countries will have an advantage, others will find the transition more difficult. Regardless of this, technological transitions do not occur in a vacuum, as they require the alignment of incentives among a multiplicity of actors, organizations and institutions, as well as the provision of complementary services and goods for the new technologies to flourish and be adopted.75 Fourth, and more important for NATO, without coordinating and cooperating on their investments in the necessary complementary assets, goods and services, Allies could find themselves having to face additional hurdles.

What types of problem could emerge? Technology-generated efficiency gains in production lead to lower prices. However, lower prices lead to increases in demand – because the relative price of substitute goods (rivals) increases.76 Over the past decade, AI – and, in particular, ML – has made a particular activity, prediction, cheaper: it is reasonable to forecast that this trend will continue in the future.77 As AI becomes cheaper, however, the demand for AI-related services will increase, thus leading to more demand for related necessities like AI specialists, AI infrastructure (and 5G networks) and AI components (processors). This in turn might well lead to scarcity and higher prices, thus pitching actors against one another – not unlike the early stages of the COVID-19 crisis, when individual self-interested actions led to collectively bad outcomes.78 In the context of a military alliance, the problem goes much deeper, as it can generate a beggar-thy-neighbour effect with allies competing for the same scarce resources.79 Moreover, without consultation and cooperation, Allies could end up developing different technological solutions, with the risk of undermining compatibility and interoperability. Similarly, they could end up prioritizing some problems over others, with the risk of developing multiple, different and redundant solutions while neglecting other points in need of attention.80 However, through intra-alliance coordination and cooperation, as well as dialogue and consultation, secondary market mechanisms and other approaches, NATO could provide an important contribution to identify and address this type of problems.81