# AI Projects AFF

## 1AC

### 1ac – Inherency

#### NATO established an AI strategic initiative but has yet to implement it – coordination, funding, and demonstration projects are still needed.

Soare ’21 (Simona, Research Fellow for Defence and Military Analysis, “Algorithmic power, NATO and artificial intelligence,” MILITARY BALANCE, 19th November 2021, https://www.iiss.org/blogs/military-balance/2021/11/algorithmic-power-nato-and-artificial-intelligence)

NATO has formally approved its first Artificial Intelligence (AI) strategy as it seeks a leading position in the adoption of AI for defence, but it may face some critical hurdles ahead in implementing the strategy, according to Simona Soare. NATO defence ministers have formally adopted the Alliance’s first artificial intelligence (AI) strategy. The document lays out six ‘baseline’ principles for ‘responsible’ military use of AI – lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation. It also provides an insight into key implementation challenges. The strategy is meant to provide a ‘common policy basis’ to support the adoption of AI systems in order to achieve the Alliance’s three core tasks – collective defence, crisis management and cooperative security. The strategy is also designed to challenge established Alliance processes for procurement, technology development and wider engagement with the private sector and academia. Only a summary of the strategy has been made public. However, it reveals four critical obstacles to implementation that NATO will face: reconciling the objectives of member nations; securing sufficient political and financial support; bridging any disconnect between the Alliance’s policy and operational units; and managing the transnational bureaucracy that will implement the strategy. Hard questions As well as being a consensus-building policy document, the strategy attempts to position NATO as the leader of AI adoption in defence. It reiterates the allies’ commitment to transatlantic cooperation on the development and use of AI in security and defence, an important element of which is ensuring inter-operability and standardisation. There are still hard questions, however, about how NATO will coordinate different national approaches to managing the development and application of AI in defence, combined with restrictions on technology use, access, sharing and transfer. For countries like the United States, it is a priority that allies agree practical guidelines for the operational use of AI-enabled systems and the necessary data-sharing, a challenge that should not be underestimated. Some allies, meanwhile, are not satisfied with the granularity of the six principles of responsible use, while others consider that overemphasising the normative approach risks ceding technological advantage to peer competitors. Similar tensions are playing out in the European Union. The EU’s proposal for an AI act is more restrictive for high-risk, high-impact applications of AI, though its impact on defence will be indirect, as it do does not apply to the military domain. In the defence realm, the European Defence Agency’s Artificial Intelligence Action Plan for Defence shares more similarities with the NATO strategy. While the plan is not public, it reportedly includes a list of use cases for military applications of AI which member states may consider for collaborative development and principles of responsible development and use. Another question that remains to be answered is the extent of NATO’s ambition to adopt AI. The strategy is meant to be implemented in a phased approach, partly to build political support for AI military projects. Initial ambitions seem modest, reportedly focusing on mission planning and support; smart maintenance and logistics for NATO capabilities; data fusion and analysis; cyber defence; and optimisation of back-office processes. As political acceptance grows and following periodic reviews of the strategy’s implementation, the goal is to also include more complex operational applications. Finally, the AI strategy runs parallel to NATO’s Military Strategy, a military-led process launched in 2019, and its Warfighting Capstone Concept, which examines alliance requirements in future operating environments. However, the AI strategy is a stand-alone document. To avoid creating narrow implementation tracks, meaningful early engagement between NATO’s policy and military communities would be beneficial to cut across any disconnect between threat-based assessments of the impact of AI on military capabilities and politically driven processes for the development and use of AI. Avoiding friction The executive summary of NATO’s AI strategy does not reflect any alignment of the roles and resources of the different NATO and national innovation bodies. It is unclear from the summary how the NATO Innovation Unit, Allied Command Transformation, the Science and Technology Organization and the NATO Communications and Information Agency will coordinate to implement the strategy. The Alliance aims to exploit AI developments in the commercial sector by adopting an open innovation model and deliberately moving away from its present procurement model. However, this will require an effort to map out the relationship between old structures, such as the NATO Industrial Advisory Group, and new engagement channels with the private sector, such as the Defence Innovation Accelerator for the North Atlantic and others created by the AI strategy. While NATO has adopted the AI strategy, there is no dedicated line of funding for it. Finance will depend on a combination of common budget funding and off-budget mechanisms such as the NATO Innovation Fund. Besides the uncertainty over the availability of funding, some Alliance agencies are concerned that their budgets could be cut and redistributed towards the implementation of the AI strategy. The allies have set a USD1 billion target for the NATO Innovation Fund. However, whether this amount is sustainably generated and distributed over the long term, and by what means, is more important for encouraging innovation than the announced figure. The promise of AI for military applications has been clear for some time; less obvious is the route to deliver on it. For all the implementation challenges it faces, the Alliance’s AI strategy represents a step in the right direction.

### 1ac – Competition Advantage

#### The AI race is on, but the US is failing behind to China – it will determine global balance of power both economically and militarily.

Franke ’21 (Ulrike Esther, senior policy fellow at the European Council on Foreign Relations (ECFR). PhD in International Relations from the University of Oxford. "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)

A Europe-US front on AI against China International competition on technology, such as 5G, has recently attracted significant attention. At the 2020 Munich Security Conference, for example, tech was an important topic – yet the discussion was not really about tech, but about power, as the rivalry over who builds 5G telecommunications infrastructure turned into a US-Chinese competition. This was despite the fact that the leading 5G providers are European and Chinese. There is a growing realisation that the adoption of AI-enabled systems may have geopolitical consequences and eventually affect the global balance of power. In particular, AI may give one actor considerable power over others, be it in the form of an economic boost or an AI-enabled military advantage, or through control over crucial technology components and standards. In the US, there is growing concern over the possibility that China might become too strong an AI actor. The competition over global leadership between the US and China is intensifying, with technology in general, and AI in particular, as battlefields. The US fears that AI may give China a competitive edge. Therefore, countering China’s AI ambitions – as embodied in its attempts to dominate international technology standards bodies, for example – has become an important motive for the US to seek international cooperation. In this context, Joe Biden has proposed an “alliance of liberal democracies” to present an economic and political alternative to China. Artificial divide: How Europe and America could clash over AI – ECFR/367 7 European policymakers have been less vocal about the geopolitical consequences of AI. So far, the debate in Europe has primarily revolved around AI’s economic and social effects. Of the 21 strategies on AI either published or drafted by EU member states, very few touch on the geopolitical implications of AI. The notable exception to this is France, whose national AI strategy was clearly drafted with a geopolitical mindset. It warns that France and Europe need to “avoid becoming just ‘digital colonies’ of the Chinese and American giants”. The strategy’s inclusion of “American giants” is telling and important. It shows that, from a European point of view, the US is the primary ‘other’ that Europe measures itself against on technology – at least for now. This is despite the fact that, in recent years, Chinese acquisitions of European high-tech firms have caused significant concern.

#### NATO is losing its technological edge – action now key to ensure future deterrence and warfighting tactics against adversaries

Jankowski ‘21 [Dominik P. Jankowski is a security policy expert, diplomat, think-tanker and social media aficionado. Currently he serves as Head of OSCE and Eastern Security Unit at the Ministry of Foreign Affairs of the Republic of Poland. Previously he served as Chief Specialist for Crisis Management at the Ministry of Foreign Affairs (2014-2016), Expert Analyst and Head of the International Analyses Division at the National Security Bureau of the Republic of Poland (2010-2014), Senior Expert at the J5-Strategic Planning Directorate of the General Staff of the Polish Armed Forces (2009-2010) as well as foreign policy expert at the President Aleksander Kwasniewski “Amicus Europae” Foundation (2007-2010). *NATO in Era of Unpeace: Defending Against Known Unknowns.* “NATO and the Emerging and Disruptive Technologies Challenge.” Pp 83-84. March 19, 2021. Lublin Publications, <https://ies.lublin.pl/wp-content/uploads/2021/03/nato-in-the-era-of-unpeace_calosc-1.pdf#page=82]//PJ>

Emerging and disruptive technologies (EDTs) seem simultaneously trendy, powerful, and mysterious. They are often perceived as carrying the potential to revolutionize governmental structures, economies, and life as one knows it. At the same time, scholars and policymakers emphasize that “these technologies may also promote international instability: for instance, by leading to a swift redistribution of wealth around the world; a rapid diffusion of military capabilities or by heightening the risks of military escalation and conflict.”1 For past decades, NATO and its Allies have enjoyed a technological edge, which has underpinned their collective military security – an advantage resulting from their collective economic, industrial, and academic strengths. NATO’s technological edge has always been an essential enabler of its ability to deter and defend against actual and potential adversaries. In October 2019, NATO Defence Ministers expressed concern that this advantage can no longer be taken for granted. In fact, NATO was in danger of losing its technological edge due to a combination of factors, among them a growing determination from peer competitors, especially Russia and China, to drive the future of advanced technologies, including military applications. Availability and knowledge of EDTs, enhanced by rising defence budgets, have provided NATO’s adversaries with capabilities to challenge the Alliance politically, militarily, and technologically. Allowing adversaries to gain competitive advantage in the EDTs area would impede NATO’s ability to win on the battlefield, challenge strategic stability, and change the fundamentals of deterrence. For NATO, EDTs are primarily of interest through their influence on current and future defence capabilities, as well as on deterrence and defence posture. It is clear that EDTs will affect many of the foundations of deterrence strategy. Indeed, new military technologies will play a crucial role in future warfighting and building forces that can decisively operate across domains. At the same time, deeply strategic and practical understanding of the significance of EDTs and their diffusion, as well as extending thinking concerning how science, technology, and international social relations interact to shape and facilitate management of the changing global security landscape, is a pressing need for NATO in the upcoming decade.2

#### Losing the AI race causes global nuclear war – multiple scenarios for Russia and China conflicts that escalate.

Kroenig & 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?,” Bulletin of the Atomic Scientists, November 12 2018,  [https://thebulletin.org/2018/11/will-disruptive-technology-cause-nuclear-war/)//akg](%20https://thebulletin.org/2018/11/will-disruptive-technology-cause-nuclear-war/)//akg)

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 tech**nology 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**.

#### Independently, lack of AI coordination wrecks overall cohesion and interoperability.

Gilli ‘20 [Andrea Gilli December 2020 “’NATO-Mation’: Strategies for Leading in the Age of Artificial Intelligence” NATO Defense College Research Paper No.15 pp. 25-28 <https://www.ndc.nato.int/download/downloads.php?icode=671>] -os-

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

#### NATO cohesion checks numerous existential crises.

Gallagher ’19 [Mike and Colin Dueck; January 2019; Representative for Wisconsin’s Eighth District in the U.S. House of Representatives; Professor in the Schar School of Policy and Government at George Mason University; National Review, “The Conservative Case for NATO,” <https://www.nationalreview.com/2019/01/nato-western-military-alliance-bolsters-american-interests/>]

The conservative case for NATO is not that it strengthens liberal world order. Rather, the conservative case for NATO is that it bolsters American national interests. In an age of great-power competition, as identified by the Trump administration, America’s Western alliance provides the U.S. with some dramatic comparative advantages. The United States, Canada, and their European allies have a number of common interests and common challenges with regard to Beijing, Moscow, terrorism, cyberattacks, migration, nuclear weapons, and military readiness. NATO is the one formal alliance that allows for cooperation on these matters. It is also the only alliance that embodies America’s civilizational ties with Europe — a point forcefully made by President Trump when he visited Poland in 2017. Properly understood, NATO helps keeps America’s strategic competitors at bay, pushing back on Russian and Chinese influence. In all of these ways, the U.S. alliance system in Europe is a bit like oxygen. You may take it for granted, but you’ll miss it when it’s gone.

#### Independently, AI enhances nuclear deterrence by improving military operations – it lifts the fog of war and improves decision making.

Nurkin and Konaev, 2022 - senior fellows at the Center for Strategy and Security at the Atlantic Council [Tate and Margarita, 5-25-2022, “Eye to eye in AI: Developing artificial intelligence for national security and defense” Atlantic Council <https://www.atlanticcouncil.org/in-depth-research-reports/report/eye-to-eye-in-ai/> ARD]

AI embodies a significant opportunity for defense policymakers. The ability of AI to process and fuse information, and to distill data into insights that augment decision-making, can lift the “fog of war” in a chaotic, contested environment in which speed is king. AI can also unlock the possibility of new types of attritable and single-use uncrewed systems that can enhance deterrence.2 It can help safeguard the lives of US service members, for example, by powering the navigation software that guides autonomous resupply trucks in conflict zones.3 While humans remain in charge of making the final decision on targeting, AI algorithms are increasingly playing a role in helping intelligence professionals identify and track malicious actors, with the aim of “shortening the kill chain and accelerating the speed of decision-making.”4 AI development and integration are also imperative due to the broader geostrategic context in which the United States operates—particularly the strategic competition with China.5 The People’s Liberation Army (PLA) budget for AI seems to match that of the US military, and the PLA is developing AI technology for a similarly broad set of applications and capabilities, including training and simulation, swarming autonomous systems, and information operations—among many others—all of which could abrogate the US military-technological advantage.6 As US Secretary of Defense Lloyd Austin noted in July 2021, “China’s leaders have made clear they intend to be globally dominant in AI by the year 2030. Beijing already talks about using AI for a range of missions, from surveillance to cyberattacks to autonomous weapons.”7 The United States cannot afford to fall behind China or other competitors.

#### Nuclear deterrence solves existential threats

Chilton 18—USAF, Retired Former commander, US Strategic Command [General Kevin P. Chilton, Spring 2018, “Defending the Record on US Nuclear Deterrence”, Strategic Studies Quarterly, <https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-1/Chilton.pdf?ver=2018-02-14-170000-437>] AMarb

Some argue the US nuclear deterrent should be eliminated because its existence represents Cold War think. If nuclear deterrence is Cold War think, then one might posit machine guns are World War I think and main battle tanks are World War II think and conclude the US does not need those anymore for the defense of the nation. In fact, nuclear deterrence is not Cold War think. The reality is nuclear deterrence underpins the national security of the United States and will continue to do so for the foreseeable future. It remains relevant and necessary today to deter the existential threats to our nation posed by both Russia and China and by lesser but certainly horrific threats posed by the Democratic People’s Republic of North Korea. It also helps to deter nonnuclear attacks that could have catastrophic consequences, such as attacks involving biological weapons. The term Cold War think is a pejorative typically proffered by those who have never thought seriously about, let alone studied, deterrence theory or by those who have run out of ways to defend their position. It is generally the last throwaway line of argument from an uninformed antinuclear ideologue. “No One Would Ever Use a Nuclear Weapon against the United States” Those who would use this argument seem willing to risk the very existence of the nation on the basis of their speculation and without forethought. However, this is not a wager military planners should ever risk. The US military must ensure national survival through deterrence provided by a safe, secure, capable, reliable, flexible, and vigilant nuclear posture. It is our duty to assume the worst and then take steps to ensure it never happens. Additionally, we must deter attacks on our friends, allies, and fielded US military forces deployed abroad. This will become more challenging as Russia, China, and North Korea appear to include the possible employment of nuclear weapons in their planning; indeed, Russia and North Korea openly discuss nuclear weapons as instruments to be used in future conventional conflicts with the US and NATO.

### 1ac – Cooperation Advantage

#### Uncertainty over AI military application puts NATO at the center of the broader debate over democracy and emerging technology – cooperation now sets international norms.

**Gilli ’20** (Andrea is Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. In the past, Andrea has been visiting and post-doctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University, “NATO-Mation”: Strategies for Leading in the Age of Artifical Intelligence,” <https://www.ndc.nato.int/about/organization.php?icode=126>, 6/25/22)-lf

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 signaling 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. Considering AI ethics also means developing trust in systems. Organizations developing AI applications should think deeply about user expectations related to transparency and disclosure. Ultimately, these norms will change the distinction between human, AI-assisted and AI interactions.101 “Calibrating” trust is especially important for AI-assisted decision making,102 a concept whose value will only increase given the emphasis on human-machine teaming in Allied militaries.103 In many cases, the unethical or unacceptable outcomes of AI systems pertain not to moral dilemmas, but to the reliability and robustness of the systems at hand. As such, building trust is fundamentally tied to building safe and secure systems.104 The problem of bias in AI illustrates the overlap between AI safety and AI ethics: bias is morally problematic, because it can unfairly harm or systematically discriminate against specific groups105 – and it can also be seen as a failure mode that reduces the reliability of a given algorithm in a given context.106 For NATO, this relates to the safety of enterprise tools and weapons systems alike. In deployments, these safety measures would be critical to ensure that AI-enabled weapons systems are used in a manner consistent with the principles of international humanitarian law. As explained in greater detail below, this may also feed into the eventual standardization process. While addressing these and other ethical issues is not impossible, it is also not immediate, especially among different actors who, understandably, may hold variegated views or priorities. Several courses of action are possible: Appoint an Ethics Board. The Atlantic Alliance could benefit from establishing an Ethics Board of experts, along the lines of the European Commission’s High-Level Expert Group on AI or the AI Ethics Committee in the French Ministry of Armed Forces. The aim should be to start an internal discussion about the applications of AI in the military domain, and the board should be empowered to monitor the progressive implementation of ethically aligned processes, principles, and standards over the medium-to-long term so as to avoid “ethics washing”.107 The board could be made of specific personalities, or also represent ethics boards already set up by individual Allies. It is important, however, that a board of this kind remains in place for the medium term: the upcoming integration of AI at entry-level will lead to new applications, and thus to wider adoption within the Alliance; for this reason, an ethics board would be increasingly called on to support trust-building measures, as well as integration of ethics into the front end of development. Similarly, it would play an important support role in providing the necessary governance for technical, moral, legal and ethical questions as the adoption of AI intensifies.108 Lead and shape with ethical principles. The proposed Ethics Board could start its work from scratch, defining a new set of guiding ethical principles for NATO and its Allies, or it could take a pragmatic approach and borrow from the important work already done by several institutions, including the OECD and the European Union.109 As recalled above, work has already been done by international organizations such as the European Union and the OECD, national governments, such as the US Department of Defense and the French Ministry of the Armed Forces, private companies like Google and IBM, as well as non-governmental institutions like the Institute for Electrical and Electronics Engineering.110 Having clear and simple ethical principles is important, both internally, as actors at different levels need to be able to make choices, and externally, as NATO and its Allies may want not only to signal their ethical and moral commitments to their own citizenries, including developers and civil society, but also to shape the international environment. The priority is to ensure that NATO Allies adopt clear ethical guidelines which reflect their values – such as democratic representation, civilian control of the armed forces, individual responsibility, the centrality of human life, and compliance with the Laws of War – and that such values inform international norms, practices, agreements and possible future treaties. Leading in this realm means moulding the future security environment, in particular by embedding democratic values into this pervasive technology.111 What ethical principles should NATO adopt when it comes to AI? This will be up to the Ethics Board, if established, or to other authorities. As recalled, there is, however, a general agreement on some principles:112 • Human centricity: AI must be based on fundamental human rights and be aimed at improving the human condition; • Safety and security: AI must be adopted and deployed in a risk management framework that accounts for and minimizes threats; • Explainability and transparency: algorithms are generally opaque. For this reason it is important that their underlying logic can be understood, and that algorithms are written in a clear way; • Responsibility and accountability: the deployment of AI must ensure that responsibility for actions can be identified, especially in the event of error, meaning that individuals or organizations can be accountable even when responsibility is distributed across many stakeholders; • Reliability: the development of AI must ensure that it is reliable, and thus does not operate unpredictably or, especially, pose unanticipated threats; • Fairness and inclusion: algorithms must be designed to improve the human condition and thus reduce bias and discrimination, not exacerbate them; and • Privacy and data governance: the privacy and sensitivity of data – with regard to individuals, equipment, processes or organizations – must be preserved and protected. Implementation and execution. The transition from principles to action is critical in any activity. Ethics is no exception, and while issuing comprehensive principles is difficult in any organisation, ensuring their implementation is an even greater challenge so as to strike the fine line between ethics washing and ethics “bashing”.113 Indeed, governance is an important factor in ensuring that technology is used responsibly and in line with the Alliance’s desired outcomes.114 In this respect, NATO may have a relevant role in supporting its Allies. A dedicated organization, such as an Artificial Intelligence Integration & Implementation-Enabling Centre (next chapter), could prove particularly useful, not least because it could help Allies share concerns, considerations, solutions and best practices as well as support them with ad hoc training activities.115 Similarly, aligned principles may eventually be translated into standards – and related measures such as benchmarks and annotations – an aspect which will be discussed towards the end of this Research Paper.

#### Plan ensures that a democratic AI model is credible – cooperation spills over to challenge the China’s authoritarianism.

**Imbrie et al. ‘20** (Andrew Imbrie, Senior Fellow at Georgetown's Center for Security and Emerging Technology; Ryan Fedasiuk, Research Analyst at Georgetown's Center for Security and Emerging Technology; Catherine Aiken, Director of Data Science and Research at Georgetown's Center for Security and Emerging Technology; Tarun Chhabra, nonresident fellow with the Center for Security, Strategy, and Technology at the Brookings Institution; Husanjot Chahal, Research Analyst at Georgetown University's Center for Security and Emerging Technology; February 2022; “HOW THE UNITED STATES AND ITS ALLIES CAN DELIVER A DEMOCRATIC WAY OF AI”; CSET; <https://cset.georgetown.edu/publication/agile-alliances/)//akg>

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. Optimal Partners: Canada, United Kingdom, Ireland, Australia, Singapore, and Japan Center for Security and Emerging Technology 33 Multilateral Fora: EU, OECD, International Organization for Standardization and International Electrotechnical Commission Joint Technical Committee 1 Sub Committee 42 – Artificial Intelligence, WTO, 3GPP, NATO-EU joint initiative on standards for emerging technologies Criteria for Partnership: To lead the global discussion on AI safety and ethics, the United States will need to build a coalition of like-minded, influential countries from which it can listen and learn and with whom it can shape norms and standards. Ideal partners will be countries that host active and engaged civil societies, who have historically aligned with liberal democratic values and U.S. policy priorities, and who most actively collaborate internationally to develop AI norms and standards. Allies that more frequently use information and communication technologies, issue governance documents about AI, and host robust public sector discussions about AI and image recognition are optimal partners for shaping global norms, standards, and best practices around these technologies. For one measure of technology use, we included the World Economic Forum’s Government Usage of ICT index, as well as a count of national AI governance documents provided by Nesta.88 We also measured commitment to a democratic way of AI by canvassing national AI strategies for mentions of “principles,” “norms,” “standards,” and “safety.” To measure international clout and diplomatic capacity, we captured the number of diplomatic posts each country operates worldwide, as well as their ranks on the Soft Power 30 Index.89 Finally, we recorded countries’ demonstrated willingness to ban technology imports from Huawei Technologies as a proxy for their willingness to work with the United States.90 Other considerations and caveats: The United States will need to expand cooperation beyond the aforementioned countries to promote liberal democratic norms and standards for AI. Sweden and New Zealand were among the top-scoring countries for this initiative. As the world’s largest democracy, India is also an important partner in this effort. Policymakers will need to weigh additional considerations: countries that generate a high quantity of policy documents about AI may not make for optimal partners if these documents do not align with U.S. values and policy priorities. What’s more, many national guidelines mention or touch on AI but are not directly related to AI, and data is not widely available for non-Anglophone countries. Initiative 10: Establish a multilateral digital infrastructure network. One of the chief attractions of Chinese-supplied consumer technologies (5G, cell phones, computers, digital wallets) is that they are less expensive than Western equivalents, and market access is often a condition for Chinese companies investing in developing countries. For example, some allies and partners are reluctant to ban Huawei for fear of losing access to the Chinese market and investments. Even among partners, the appeal of cost effectiveness sometimes outweighs considerations of privacy and security. The CSET survey found that cost effectiveness matters more than privacy for international agreements around software contracts. Yet privacy matters more among partners for international agreements around data storage and sharing. Surveyed officials were split in terms of the relative importance of privacy and cost for international agreements around novel applications and hardware investment. Germany, Australia, and the EU tended to favor privacy in all cases, while Colombia and the Czech Republic tended to favor cost effectiveness when considering international collaboration. To promote a rules-based global trading order, the United States should not mimic China’s model of state-driven, top-down national development strategies that trade investment for market access. Instead, the United States should form a multilateral consortium to coordinate the extension of credit to European mobile telecommunications networks and invest in next-generation networks.91 The United States and its allies should also launch a multilateral digital infrastructure network. This network could be modeled on USAID’s Higher Education Solutions Network, a partnership between USAID and development labs at seven major universities, and the EU’s Digital4Development policy, an initiative that harnesses information and communications technologies to promote sustainable development.92 A multilateral digital infrastructure network would enable the United States and its allies to partner with developing countries to build digital capacity in support of the UN’s Sustainable Development Goals. The right approach would ensure that digital systems in emerging markets are open, secure, resilient, and interoperable, while empowering developing countries to protect data privacy, meet their domestic needs, and access high-performance computing and mobile internet technologies. Liberal democratic governments have established frameworks and standards for good governance tied to development lending and giving. Democratic countries should include AI in these frameworks along with capacity building to ensure that developing countries can make sovereign and democratically accountable decisions about the deployment of AI. Many developing countries are growth markets and present opportunities to shape AI governance consistent with liberal democratic principles. As part of this effort, the United States and its allies should integrate federated learning techniques and data privacy into digital capacity building efforts with developing countries. By creating an accelerator fund for privacy-preserving 36 Center for Security and Emerging Technology machine learning technologies, the United States and its allies could promote an alternative model of development that puts data protection and privacy at the absolute center. Optimal Partners: Germany, Japan, France, United Kingdom, Ireland, and Canada Multilateral Fora: IMF, World Bank, European Bank for Reconstruction and Development, Asian Development Bank, and Digital Nations (The Digital 9) Criteria for Partnership: The best partners for investing in global digital infrastructure are countries that lead in foreign aid and consider technology to be a staple of development and governance. We measured outflows of official development assistance (ODA) and foreign direct investment (FDI) from each country. We considered three indices of governments’ commitment to technology and global development: the UN e-Government Development Index, the Digital Evolution Index, and “technology” scores on the Commitment to Development Index.93 We also included a measure from our survey: expressed concern around China’s investments in the developing world. Other considerations and caveats: Other high-scoring countries included South Korea and Sweden for their commitments to digital development. It is also important to consider the optimal destinations for digital infrastructure support. Ideal recipients would be countries at risk of becoming dependent on Chinese technology and monetary assistance, for whom price is a prohibitory factor in buying from companies based in the United States and allied countries. As of this writing, China’s Belt and Road Initiative encompasses more than 60 countries.94 Conclusion 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.

#### Chinese dominance of AI spread authoritarianism globally – subjects billions to state-sponsored violence.

Anderson ‘20 (Ross Andersen is a senior editor at The Atlantic, where he oversees the science, technology, and health sections. He joined The Atlantic in 2015. He was previously the deputy editor of Aeon, and before that, he was the science editor of the Los Angeles Review of Books. In addition to his work as an editor, Andersen is known for his award-winning feature essays, which straddle philosophy, technology, science, history, and the arts.) “THE PANOPTICON IS ALREADY HERE” September 2020 <https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/> // ZX

The lobby’s most prominent poster depicted Xi Jinping in a crisp black suit. China’s current president and the general secretary of its Communist Party has taken a keen interest in the institute. Its work is part of a grand AI strategy that Xi has laid out in a series of speeches akin to those John F. Kennedy used to train America’s techno-scientific sights on the moon. Xi has said that he wants China, by year’s end, to be competitive with the world’s AI leaders, a benchmark the country has arguably already reached. And he wants China to achieve AI supremacy by 2030. Xi’s pronouncements on AI have a sinister edge. Artificial intelligence has applications in nearly every human domain, from the instant translation of spoken language to early viral-outbreak detection. But Xi also wants to use AI’s awesome analytical powers to push China to the cutting edge of surveillance. He wants to build an all-seeing digital system of social control, patrolled by precog algorithms that identify potential dissenters in real time. China’s government has a history of using major historical events to introduce and embed surveillance measures. In the run-up to the 2008 Olympics in Beijing, Chinese security services achieved a new level of control over the country’s internet. During China’s coronavirus outbreak, Xi’s government leaned hard on private companies in possession of sensitive personal data. Any emergency data-sharing arrangements made behind closed doors during the pandemic could become permanent. China already has hundreds of millions of surveillance cameras in place. Xi’s government hopes to soon achieve full video coverage of key public areas. Much of the footage collected by China’s cameras is parsed by algorithms for security threats of one kind or another. In the near future, every person who enters a public space could be identified, instantly, by AI matching them to an ocean of personal data, including their every text communication, and their body’s one-of-a-kind protein-construction schema. In time, algorithms will be able to string together data points from a broad range of sources—travel records, friends and associates, reading habits, purchases—to predict political resistance before it happens. China’s government could soon achieve an unprecedented political stranglehold on more than 1 billion people. Early in the coronavirus outbreak, China’s citizens were subjected to a form of risk scoring. An algorithm assigned people a color code—green, yellow, or red—that determined their ability to take transit or enter buildings in China’s megacities. In a sophisticated digital system of social control, codes like these could be used to score a person’s perceived political pliancy as well. A crude version of such a system is already in operation in China’s northwestern territory of Xinjiang, where more than 1 million Muslim Uighurs have been imprisoned, the largest internment of an ethnic-religious minority since the fall of the Third Reich. Once Xi perfects this system in Xinjiang, no technological limitations will prevent him from extending AI surveillance across China. **He could also export it beyond the country’s borders, entrenching the power of a whole generation of autocrats.**China has recently embarked on a number of ambitious infrastructure projects abroad—megacity construction, high-speed rail networks, not to mention the country’s much-vaunted Belt and Road Initiative. But these won’t reshape history like China’s digital infrastructure, which could shift the balance of power between the individual and the state worldwide. American policy makers from across the political spectrum are concerned about this scenario. Michael Kratsios, the former Peter Thiel acolyte whom Donald Trump picked to be the U.S. government’s chief technology officer, told me that technological leadership from democratic nations has “never been more imperative” and that “if we want to make sure that Western values are baked into the technologies of the future, we need to make sure we’re leading in those technologies.” Despite China’s considerable strides, industry analysts expect America to retain its current AI lead for another decade at least. But this is cold comfort: **China is already developing powerful new surveillance tools, and exporting them to dozens of the world’s actual and would-be autocracies**. Over the next few years, those technologies will be refined and integrated into all-encompassing surveillance systems that dictators can plug and play. The emergence of an AI-powered authoritarian bloc led by China could warp the geopolitics of this century. It could prevent billions of people, across large swaths of the globe, from ever securing any measure of political freedom. And whatever the pretensions of American policy makers, only China’s citizens can stop it. I’d come to Beijing to look for some sign that they might. Xi has appropriated the phrase sharp eyes, with all its historical resonances, as his chosen name for the AI-powered surveillance cameras that will soon span China. With AI, Xi can build history’s most oppressive authoritarian apparatus, without the manpower Mao needed to keep information about dissent flowing to a single, centralized node. In China’s most prominent AI start-ups—SenseTime, CloudWalk, Megvii, Hikvision, iFlytek, Meiya Pico—**Xi has found willing commercial partners. And in Xinjiang’s Muslim minority, he has found his test population.** By 2009, China’s Uighurs had become weary after decades of discrimination and land confiscation. They launched mass protests and a smattering of suicide attacks against Chinese police. In 2014, Xi cracked down, directing Xinjiang’s provincial government to destroy mosques and reduce Uighur neighborhoods to rubble. More than 1 million Uighurs were disappeared into concentration camps. Many were tortured and made to perform slave labor. Uighurs who were spared the camps now make up the most intensely surveilled population on Earth. Not all of the surveillance is digital. The Chinese government has moved thousands of Han Chinese “big brothers and sisters” into homes in Xinjiang’s ancient Silk Road cities, to monitor Uighurs’ forced assimilation to mainstream Chinese culture. They eat meals with the family, and some “big brothers” sleep in the same bed as the wives of detained Uighur men. Until recently, it was difficult to imagine how China could integrate all of these data into a single surveillance system, but no longer. In 2018, a cybersecurity activist hacked into a facial-recognition system that appeared to be connected to the government and was synthesizing a surprising combination of data streams. The system was capable of detecting Uighurs by their ethnic features, and it could tell whether people’s eyes or mouth were open, whether they were smiling, whether they had a beard, and whether they were wearing sunglasses. It logged the date, time, and serial numbers—all traceable to individual users—of Wi-Fi-enabled phones that passed within its reach. It was hosted by Alibaba and made reference to City Brain, an AI-powered software platform that China’s government has tasked the company with building. City Brain is, as the name suggests, a kind of automated nerve center, capable of synthesizing data streams from a multitude of sensors distributed throughout an urban environment. Many of its proposed uses are benign technocratic functions. Its algorithms could, for instance, count people and cars, to help with red-light timing and subway-line planning. Data from sensor-laden trash cans could make waste pickup more timely and efficient. In the early aughts, the Chinese telecom titan ZTE sold Ethiopia a wireless network with built-in backdoor access for the government. In a later crackdown, dissidents were rounded up for brutal interrogations, during which they were played audio from recent phone calls they’d made. Today, Kenya, Uganda, and Mauritius are outfitting major cities with Chinese-made surveillance networks. In Egypt, Chinese developers are looking to finance the construction of a new capital. It’s slated to run on a “smart city” platform similar to City Brain, although a vendor has not yet been named. In southern Africa, Zambia has agreed to buy more than $1 billion in telecom equipment from China, including internet-monitoring technology. China’s Hikvision, the world’s largest manufacturer of AI-enabled surveillance cameras, has an office in Johannesburg. Having set up beachheads in Asia, Europe, and Africa, China’s AI companies are now pushing into Latin America, a region the Chinese government describes as a “core economic interest.” China financed Ecuador’s $240 million purchase of a surveillance-camera system. Bolivia, too, has bought surveillance equipment with help from a loan from Beijing. Venezuela recently debuted a new national ID-card system that logs citizens’ political affiliations in a database built by ZTE. In a grim irony, for years Chinese companies hawked many of these surveillance products at a security expo in Xinjiang, the home province of the Uighurs. The country is now the world’s leading seller of AI-powered surveillance equipment. In Malaysia, the government is working with Yitu, a Chinese AI start-up, to bring facial-recognition technology to Kuala Lumpur’s police as a complement to Alibaba’s City Brain platform. Chinese companies also bid to outfit every one of Singapore’s 110,000 lampposts with facial-recognition cameras.

#### 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.

### 1ac – Plan

#### The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization over artificial intelligence-enabled military logistics and sustainment projects.

### 1ac – Solvency

#### Security cooperation for AI logistics and sustainment projects solves – it improves alliance interoperability, military readiness, and leads to quick innovation. US leadership, within NATO, counters adversaries and locks in a democratic AI model.

Konaev & Chahal ’21 (Margarita Konaev is a research fellow with CSET, where Husanjot Chahal is a research analyst. "The Path of Least Resistance Multinational Collaboration on AI for Military Logistics and Sustainment" April, Center for Security and Emerging Technology, Georgetown University, https://cset.georgetown.edu/wp-content/uploads/CSET-Path-of-Least-Resistance.pdf)

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 is key – focusing on non-controversial security cooperation sets a model for broader cooperation – US leadership is also key.

Franke ’21, (Ulrike Esther Franke, senior policy fellow at the European Council on Foreign Relations, PhD in International Relations from the University of Oxford. “ARTIFICIAL DIVIDE: HOW EUROPE AND AMERICA COULD CLASH OVER AI,” ECRF, January 2021, <https://ecfr.eu/wp-content/uploads/Artificial-divide-How-Europe-and-America-could-clash-over-AI.pdf>)

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. CONCLUSION This paper has discussed the rationale for transatlantic cooperation on AI. It has shown that both Europe and the US have reasons for wanting to cooperate with each other. But substantial hurdles may prevent the transatlantic partners from cooperating in a significant way. However, they can still look to ramp up their cooperation. And non-combat military AI, in particular, may be low-hanging fruit for AI cooperation within NATO. Europeans should reach out to their American allies, so that a new, third phase of Europe’s policy efforts in this AI spring can indeed become a phase of international – and particularly transatlantic – cooperation.

## Inherency

### AT: SQ Solves

#### NATO is key for ensuring a western AI advantage BUT requires further guidelines and investment since its 2021 declaration.

Christie and Ertan 22 (Edward Hunter Christie is the owner and founder of AI Policy Consulting. He served as a NATO official from 2014 to 2020, ending his tenure in the role of Deputy Head of NATO’s Innovation Unit. Amy Ertan is a cybersecurity fellow at the Belfer Center for Science and International Affairs (Harvard Kennedy School), researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and doctoral candidate at the Information Security Group, Royal Holloway, University of London.) “NATO and Artificial Intelligence” 14 Jun 2022 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4133397> // ZX

NATO is a military alliance of democratic states in the North Atlantic region. Its first essential core task, unchanged since the Alliance’s creation in 1949, is collectively to deter and if necessary defend against armed attacks against any one of its members in the North Atlantic region, in line with Article 51 of the United Nations Charter. To ensure this primary task, Allied governments coordinate their defence policies to ensure a chosen degree of collective military interoperability, capability, and readiness. This is pursued through activities such as the definition and implementation of common military-technical standards, of commonly agreed military capability targets, and of common capability development activities and projects. At the organisational level, NATO has a permanent common military command structure which enables it, among other tasks, to uphold readiness, to organise exercises, and to lead collective military operations following relevant political decisions. NATO also pursues two additional core tasks in addition to collective defence, namely crisis management and cooperative security1, which leverage NATO’s nature and purpose as a military alliance. NATO’s purpose and structures imply a centrality of military considerations in how it approaches any new security challenge. NATO decisions are taken by consensus among Allied governments, through a multi-layered hierarchy of committees. The most senior committee, the North Atlantic Council (NAC), is a civilian committee. The NAC meets regularly at the level of Ambassadors, four times a year at the Ministerial level (twice Defence Ministers, twice Foreign Ministers), and on average every two years at the level of Heads of State and Government. In practice, NATO’s activities include consultations among Allied governments on matters of common interest, ranging from broad strategic discussions on international security developments to detailed decision-making on particular activities, projects, standards, targets, or policies. Warfare has always been shaped by technology. Artificial intelligence has already demonstrated the potential to enhance military capabilities and to create new military capabilities. From intelligence, surveillance and reconnaissance to inclusion in unmanned systems, or across logistics and support functions, there are a number of consequences of AI inclusion across military domains that warrant attention and activity from NATO as an Alliance and as an organization. As noted by the STO, AI “has the potential for revolutionary impact on NATO operations and capabilities”, describing AI as a “fulcrum around which big data will be turned into actionable knowledge, and, ultimately, a NATO decision advantage” (2020, p.14). The STO further notes that “integration of AI into combat models & simulation, enterprise systems, decision support systems, cyber defence systems and autonomous vehicles will allow for rapid and more effective human-machine decision making” (2020, p.15). The formulation of AI policies for the area of defence is a recent but fast-moving area of work. At the time of writing, the United States and France were the only Allies with published national AI defence strategies (US Department of Defense, 2018; French Ministry of the Armed Forces, 2019), with the UK announcing their intention to release a defence-focused AI strategy, see UK Ministry of Defence (2021: p.42), likely before the end of 2021. At NATO, the International Staff produced two policy White Papers for the consideration of Allied governments in the course of 2020, one on Artificial Intelligence, the other on Autonomous Technologies more specifically. In October 2021, NATO Defence Ministers approved NATO’s first-ever AI Strategy, as well as a related Data Exploitation Policy (NATO, 2021a). These policy documents will be discussed in sections 4 and 5 below, with a main focus on the AI Strategy. Iterative development refers to the fact that software development in general, and AI development in particular, requires highly iterative and dynamic work processes that are generally referred to as Agile development. From a project management perspective, traditional development generally follows a Waterfall model, a linear process where each step is completed before moving on to the next step. Agile development, by contrast, allows for development steps to be revisited and adjusted multiple times in a more dynamic manner, with much shorter development and testing timelines. The need to adopt Agile development approaches is well understood in key parts of the NATO Enterprise, notably Allied Command Transformation (ACT) and the NATO Communications and Information Agency (NCIA), and in many national defence institutions. What is less clear is what types of reforms need to be enacted at higher organisational levels. Access to data refers to a range of organisational and normative challenges to ensure that Allied defence institutions can leverage the data they have as effectively as possible. To address these challenges, a NATO Data Exploitation Policy was developed, based on detailed consultations with internal NATO Enterprise stakeholders and with representatives of Allied governments. The Policy is based on the recognition of the need for a comprehensive life-cycle approach to data resources (including collection, documentation, storage, exploitation, retention, and disposal) and for the further development of relevant enabling factors for each lifecycle stage. NATO’s emerging data policy efforts also include the formulation of guiding principles that partly mirror the principles of responsible use that should hold for AI, with the addition of specific considerations that relate to data ownership and management. To the extent that the NATO Enterprise carries out its own data exploitation and AI development efforts, the relevant NATO staffs will need the relevant structures, resources, and staff to do so, in a manner that mirrors what occurs in national defence institutions. Additional considerations are necessary to ensure that the NATO Enterprise can play a full role as a facilitator for common multinational and Alliance-wide efforts. A particularly salient issue in that context is the collaborative training of Machine Learning algorithms. While individual Allies may choose in many cases to remain the sole owners and custodians of the real-world military data they collect, there is a good case for seeking economies of scale and scope through collaborative data exploitation and algorithm training efforts. Intuitively, one may expect this to imply a need to pool datasets from multiple institutions under the custodianship of a single entity, for example a NATO body. This need not necessarily be the case, thanks to the existence of technical solutions that allow for the collaborative development of Machine Learning algorithms based on sharing successive trained instances of algorithms without actual data pooling. However, significant practical work will be necessary to ensure that the Alliance is able to pursue both types of effort – informally, data sharing versus model sharing – in efficient and seamless ways

#### NATO 2021 guidelines are a good starting point but agency, funding, and sufficient infrastructure are required to guide AI towards ethical development.

Christie and Ertan 22 (Edward Hunter Christie is the owner and founder of AI Policy Consulting. He served as a NATO official from 2014 to 2020, ending his tenure in the role of Deputy Head of NATO’s Innovation Unit. Amy Ertan is a cybersecurity fellow at the Belfer Center for Science and International Affairs (Harvard Kennedy School), researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and doctoral candidate at the Information Security Group, Royal Holloway, University of London.) “NATO and Artificial Intelligence” 14 Jun 2022 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4133397> // ZX

The practical adoption of AI presents certain challenges for Allied defence institutions. Christie (2021) identifies four areas to consider: iterative development, access to human capital, access to data, and engagement with civilian-oriented technology institutions through supportive innovation mechanisms. Iterative development refers to the fact that software development in general, and AI development in particular, requires highly iterative and dynamic work processes that are generally referred to as Agile development. From a project management perspective, traditional development generally follows a Waterfall model, a linear process where each step is completed before moving on to the next step. Agile development, by contrast, allows for development steps to be revisited and adjusted multiple times in a more dynamic manner, with much shorter development and testing timelines. The need to adopt Agile development approaches is well understood in key parts of the NATO Enterprise, notably Allied Command Transformation (ACT) and the NATO Communications and Information Agency (NCIA), and in many national defence institutions. What is less clear is what types of reforms need to be enacted at higher organisational levels. Access to data refers to a range of organisational and normative challenges to ensure that Allied defence institutions can leverage the data they have as effectively as possible. To address these challenges, a NATO Data Exploitation Policy was developed, based on detailed consultations with internal NATO Enterprise stakeholders and with representatives of Allied governments. The Policy is based on the recognition of the need for a comprehensive life-cycle approach to data resources (including collection, documentation, storage, exploitation, retention, and disposal) and for the further development of relevant enabling factors for each lifecycle stage. NATO’s emerging data policy efforts also include the formulation of guiding principles that partly mirror the principles of responsible use that should hold for AI, with the addition of specific considerations that relate to data ownership and management. To the extent that the NATO Enterprise carries out its own data exploitation and AI development efforts, the relevant NATO staffs will need the relevant structures, resources, and staff to do so, in a manner that mirrors what occurs in national defence institutions. Additional considerations are necessary to ensure that the NATO Enterprise can play a full role as a facilitator for common multinational and Alliance-wide efforts. A particularly salient issue in that context is the collaborative training of Machine Learning algorithms. While individual Allies may choose in many cases to remain the sole owners and custodians of the real-world military data they collect, there is a good case for seeking economies of scale and scope through collaborative data exploitation and algorithm training efforts. Intuitively, one may expect this to imply a need to pool datasets from multiple institutions under the custodianship of a single entity, for example a NATO body. This need not necessarily be the case, thanks to the existence of technical solutions that allow for the collaborative development of Machine Learning algorithms based on sharing successive trained instances of algorithms without actual data pooling. However, significant practical work will be necessary to ensure that the Alliance is able to pursue both types of effort – informally, data sharing versus model sharing – in efficient and seamless ways. Allied governments should also consider increasing public funding levels for research & development in AI and related technologies, as well as enhancing collaborative public-private financing mechanisms to support technological innovation at various stages of maturity. To support these goals, two major initiatives championed by NATO’s Innovation Unit were approved by Allies in 2021, namely the creation of a Defence Innovation Accelerator for the North Atlantic (DIANA) and the launch of a NATO Innovation Fund (NATO, 2021c). The versatility and adaptability of AI technologies pose specific challenges in terms of governance. A large volume of analysis and commentary has already been devoted to ethical considerations, leading to the adoption by many organisations of a range of principles. In the course of 2021, NATO developed and negotiated its first-ever AI Strategy. The final text as approved by Allies was formally agreed by Allied Defence Ministers in October 2021. A summary of the Strategy was released to the public, consistent with the stated aim of the Alliance “to lead by example and encourage the development and use of AI in a responsible manner” (NATO, 2021). The Strategy and its summary contain a set of Principles of Responsible Use which were closely modelled on the DoD principles and other existing national principles. The NATO Principles constitute a political commitment that applies to both the Alliance and the NATO Enterprise (the expression “Allies and NATO” is used in the text), in other words it is also a commitment by each national government regarding its national activities, regardless of whether they are intended for NATO activities or for national or other multinational activities outside of the NATO context. As in the DoD case, the NATO principles “apply across all types of AI applications” (NATO, 2021). An additional issue on the scope of application which is clearer in the NATO case is that the principles apply to “the AI applications they [Allies and NATO] develop and consider for deployment” (NATO, 2021). By implication, AI applications that are not intended for deployment could deviate from the principles. The underlying reasoning for this caveat is to allow for experimental applications or systems that entail deviations from principles that are necessary, for example for the development of countermeasures against actual or hypothetical adversarial capabilities that do not conform to the principles or for enhancing understanding of the technical characteristics necessary to ensure compliance with all principles. A process of learning-by-doing will be necessary across Allied defence institutions and relevant NATO bodies in order to operationalise NATO’s Principles of Responsible Use. Over time and based on experience in the implementation of the principles, Allies and NATO should be able to formulate with greater precision how the principles are to be applied, potentially leading to new NATO military-technical standards, to reliance on emerging civilian technical standards where that is more efficient, and to new or updated certification processes. In that context, the development of relevant review methodologies and of risk and impact assessment frameworks, and relevant updates to security certification requirements will be important (Stanley-Lockman and Christie, 2021). NATO’s cooperative structures and consultation mechanisms will provide a basis for the testing, evaluation, validation and verification (TEVV) of AI-enabled capabilities against intended use cases and the NATO Principles of Responsible Use. Ongoing applied research within the NATO Science & Technology Organisation’s networks on matters such as human-machine teaming, and machine-machine and humans ystems integration, among others, will provide essential contributions (Stanley-Lockman and Christie, 2021). Existing and emerging national and NATO test centres, most likely including those foreseen under NATO’s Defence Innovation Accelerator for the North Atlantic (DIANA), will be instrumental in the operationalisation of the Principles of Responsible Use by providing facilities, personnel, and procedures for relevant TEVV and certification activities. This would include a range of simulation and modelling activities, in addition to physical testing as appropriate. Focusing on the technical characteristics to be ensured during the design and development phases, it is important to note that AI applications pose challenges in terms of testing and validation. A simple mechanical device can be subject to relatively simple testing protocols to ensure its safety, and such testing protocols, while informed by practical uses, can be standardised to a high degree. AI applications, on the other hand, are too versatile, changeable, and context-dependent to allow for an ex-ante formulation of all possibly relevant technical tests. Instead, the way forward is to design and apply adequate “methodological standards” on the processes inherent to the design and development of AI algorithms, rather than on each trained instantiation of every AI algorithm. Allies and NATO have laid important policy foundations for the military use of AI. A particularly visible development is the adoption, by the United States in 2020 and by the entire NATO Alliance in 2021, of principles of responsible development and use. This is only the beginning of a long process of technological transformation, adoption, and adaptation. Multiple challenges have been identified that need to be addressed in order to adopt AI and leverage data as a strategic resource. Looking across the range of organisational, institutional, human resources, and investment challenges, one evident general conclusion is that Allied governments will need to mobilise new and greater financial resources and hire new staff and train existing staff if they wish to adopt and adapt as required. At the same time, relevant policy adaptation should accompany this process, on the one hand to directly support technology adoption, and on the other hand to ensure good governance and responsible use. The latter topic is generally the most analysed and discussed in policy communities, both inside and outside government. In this chapter, we wished to stress that this most popular topic has already moved beyond the general discussion phase and is now in need of technical layers of additional work to ensure that recently adopted principles are implemented in practice.

### AI Not Developed Yet

#### More NATO AI Projected needed.

Sanur Sharma May 30, 2022 [ Associate Fellow at Manohar Parrikar Institute for Defence Studies and Analyses.; NATO’s AI Push And Military Implications – Analysis; EurasiaReview]

The influence of AI on NATO comes with a set of opportunities, challenges and risks. Its adoption process has been incremental and prescriptive. The rising geopolitical conflicts and the use of AI in such conflicts have required the establishment of a dynamic ecosystem to support interoperability. The military adoption of AI requires an innovation ecosystem that is self-sufficient, supports deterrence and resilience, and encompasses the strategic innovation process. NATO’s AI strategy raises many concerns related to the AI-driven autonomous weapon systems, as it does not adequately address the development of such systems, its deployment and governance. The AI strategy mostly talks about the ethical and responsible use of AI and has omitted the challenges related to the use of lethal autonomous weapon systems. For the US, its priorities lie in ensuring responsible use of AI-enabled systems with their allies for operational and data sharing. It remains to be seen if all the 30 NATO states agree on the same rules and would be willing to agree on practical guidelines for the operational use of AI-enabled systems. Another challenge for NATO is to standardise rules for all member states in dealing with AI-enabled autonomous weapon systems. Countries like Turkey are working on autonomous weapons and have developed AI-enabled loitering munitions. Turkey has requested the US for upgraded F-16 fighter jets that are said to be AI-enabled.25 The Biden Administration has asked the Congress to approve the upgrade of Turkey’s F-16 fighter jet fleet.26 Turkey’s armed drones have also been used in the Ukraine conflict. For smooth functioning of such systems, it will be necessary for all NATO members to have standardised rules when it comes to deployment of such systems. Also, there is no transparent allocation of roles for different NATO bodies, and “no dedicated line of funding” for its AI strategy.27 The finances are shared through multiple funding like NATO Innovation Fund and DIANA which manages funding for various other projects leading to uncertainty over availability of funds and budget cuts. This will be a significant challenge for the effective implementation of the AI strategy.28 Some other challenges with the adoption of AI strategy through innovation include fragmented national innovation initiatives, allied technological categorisation and digitisation gaps, speed of adoption and spending levels and the underuse of NATO’s mechanisms to undertake collaborative defence innovation.29 NATO will also have to focus on the vulnerabilities and intrusion issues with the AI-enabled systems and will need to set up dedicated centres for AI development and testing in order to maintain a test-safety regime for systems-of-systems employed using AI. The challenges related to AI use in wars and geopolitical conflicts need to be addressed to generate confidence in the use of such systems. Additionally, testing mechanisms and accuracy standards need to be implemented for system components. Policymakers need to address the operational risks and ethical considerations of employing AI in military systems. In future, AI will act as an enabler to out-adapt competitors and adversaries. The current AI strategy of NATO needs to address the vulnerabilities in AI systems and related measures for effectively using autonomous weapon systems and military governance of AI. The NATO accelerator has been devised to address, prioritise, and promote interoperability in transatlantic cooperation to drive the strategic innovation process. The key drivers for Innovation in AI and other EDTs will be the establishment of the NATO-Civil-Military Technology capability that will include various actors from the military, civil, state and private sectors as a part of the EDT innovation ecosystem. Another critical factor is the broadening of the NATO–EU cooperation through a joint taskforce on defence innovation and EDTs to regularise and provide strategic capabilities on ethical and adoption challenges of EDTs like AI and ML. Furthermore, NATO needs to protect the use of AI from manipulation and disruption and align it with its stated principle of “Responsible use of AI”. NATO needs to work on AI adoption challenges centred on innovation and arms control. It can look towards bringing in guiding principles on use of AI-driven lethal autonomous weapon systems. It is expected that in the next 2–3 years, AI’s use will be confined to the field of military logistics, reconnaissance, mission planning and support, predictive maintenance of a military facility, data fusion and analysis, cyber defence and optimisation of processes. In the long run, NATO could employ AI for more complex military applications as it generates greater political support for offensive AI military projects.

## Competition Advantage

### AI Race Now

#### AI development is coming and inevitable. Only effective management and regulation can prevent widespread collapse of deterrence postures.

Diwakar 21 (Amar Diwakar is an independent writer and researcher. He has written for Al Jazeera English, The Boston Globe, In These Times, and other publications.) 17 JUN 2021 “The future of war and deterrence in an age of autonomous weapons” [https://www.trtworld.com/magazine/the-future-of-war-and-deterrence-in-an-age-of-autonomous-weapons-47602 //](https://www.trtworld.com/magazine/the-future-of-war-and-deterrence-in-an-age-of-autonomous-weapons-47602%20//) ZX

Artificial intelligence and autonomous systems will significantly alter the future battlefield and challenge strategists to come up with new models of deterrence. Innovation in the field of emerging technologies – broadly encompassing developments such as artificial intelligence (AI), robotics, drones, quantum computing, 3D printing, biotech – is evolving at breakneck speed with the potential to have far-reaching consequences on everything from governance and commerce to geopolitics. When it comes to warfare, many of these critical technologies possess the power to completely upend the terms of human conflict and alter future battlefields. “AI and robotics will smash the status quo that exists in the world today,” geopolitical futurist Abishur Prakash told TRT World, adding that new technologies will “reduce the gap between advanced military powers and the rest of the world”. With traditional concepts of state power gradually intertwined with national expertise and investment in AI, a [global arms race](https://www.weforum.org/agenda/2021/02/heres-what-you-need-to-know-about-the-new-ai-arms-race/) is already underway, with the US and China at the forefront. As wider adoption accelerates, conventional notions around deterrence are set to come into question too. What happens to deterrence and escalation when decisions can be made at machine speeds and are carried out by forces that do not risk human lives? “We will need to rethink the central tenets of deterrence. AI and autonomous systems challenge the way that nuclear and non-nuclear operations are conducted, as well as the way these systems can be held vulnerable to attack,” says Mikhail Sebastian, a London-based political risk analyst specialising in cybersecurity and digital diplomacy. “At the same time, they offer a new suite of options for deterring nuclear attacks.” Prakash warns we’ve now reached a point of no return. “We are exiting the era where the most damaging behaviour could be deterred. Now, as technology gives nations and organisations new capabilities, governments are faced with threats they cannot stop or limit,” he says. “They can only be managed.” Autonomous battlefields If there is one military technology proven to be a gamechanger thus far, it’s drones. After gunpowder and nuclear weapons, many have referred to automated killer robots as the “[third revolution in warfare](https://www.bbc.com/news/technology-40995835)”. Late last year amid the pandemic, the Second Nagorno-Karabakh War between Azerbaijan and Armenia amounted to a showcase for autonomous weapons – and provides a glimpse of the battlefield of the future. Azerbaijan deployed a range of drones, purchased from Israel and Turkey, to rout the otherwise conventionally superior Armenian army in a short space of time. Azeri forces used to [devastating effect](https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html) Israeli-made ‘Harop’ loitering munitions, designed to hover high above the battlefield while waiting to be assigned a target to crash their explosive payload into, earning them the moniker “[Kamikaze drones](https://www.rferl.org/a/nagorno-karabakh-kamikaze-drone-debut/27658645.html)”. Azerbaijan spent years investing in loitering munitions and accumulated a stock of over 200, while Armenia had only one domestically made model with a limited range. Being the first war won by autonomous weapons, an [uptick in interest](https://www.theguardian.com/world/2020/dec/29/uk-defence-secretary-hails-azerbaijans-use-of-drones-in-conflict) from national armies acquiring unmanned aerial systems followed shortly after. In the US, a new [report](https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf) from the National Security Commission on AI discusses how autonomous technologies are enabling a new paradigm in warfighting and urges massive amounts of investment in the field. Countries are intensely [competing](https://www.foreignaffairs.com/articles/china/2020-11-20/china-has-made-drone-warfare-global) to build or purchase cutting-edge drone systems: China and Russia intend to pursue the development of autonomous weapons and are investing heavily in R&D. The UK’s new defence strategy puts AI front and centre, as does Israel. And a much more transformative drone technology could be just on the horizon. Advances in Li-ion batteries have given rise to cheaply made miniature quadcopters. Multiple air forces are now beginning to test networked [swarms of drones](https://www.thedrive.com/the-war-zone/36950/raf-tests-swarm-loaded-with-britecloud-electronic-warfare-decoys-to-overwhelm-air-defenses) that can overwhelm radar systems. Sebastian points out that while on its own a single unmanned and autonomous unit is no match for a fighter jet, when algorithmically linked together a fleet of thousands can conceivably overwhelm larger platforms. “Once refined, low-cost autonomous drones coordinating their actions at machine speed provide a unique coercive tool that undermines high-cost legacy weapon systems, while potentially augmenting the feasibility of an offensive attack,” he told TRT World. Possibly the scariest development are autonomous quadcopters equipped with computer vision technology that can recognise and kill a specific target, or so-called [assassination drones](https://www.businessinsider.com/killer-drone-hunted-down-human-target-without-being-told-un-2021-5). “As opposed to other military drone applications, assassin drones don’t have to be confined to the battlefield. They can lurk as an omnipresent threat outside of wartime,” says Sebastian. Until now, deterrence has primarily involved humans attempting to affect the decision calculus and perceptions of other humans. But what happens when decision-making processes are no longer fully under human control? ‘How does one deter an event that has not happened yet?’ What sets the new technology arms race apart from the past is AI’s dual-use. During the Cold War, the development of nuclear weapons was driven by governments and the defence industry. Beyond power generation, there wasn’t much commercial use for nuclear technology. But that model doesn’t apply anymore. “The creeping ubiquity of AI means developments in technologies cannot be contained, and they are bound to bleed across the civilian and military realms,” Sebastian notes. In an [article](https://www.tandfonline.com/doi/full/10.1080/14751798.2020.1857911) published last year James Johnson, an assistant professor in the School of Law and Government at Dublin City University, argued the dual-use and diffused nature of AI compared to nuclear technology will make arms control efforts problematic. “When nuclear and non-nuclear capabilities and war-faring are blurred, strategic competition and arms racing are more likely to emerge, complicating arms control efforts,” he wrote. “In short, legacy arms control frameworks, norms, and even the notion of strategic stability itself will increasingly struggle to assimilate and respond to these fluid and interconnected trends.” Johnson underscores what is now referred to as the nascent “fifth wave” of modern deterrence (the “fourth wave” followed the Cold War and continues to the present, coinciding with multipolarity, asymmetric threats and non-state actors) is defined by a conceptual break by including non-human agents into deterrence. It then follows that asymmetric AI capabilities will inform deterrence strategies. To fight autonomous weapons, you need those same weapons – driving actors to adopt these technologies to shore up their defence against autonomous attacks. The mix of human and artificial agents could affect escalation between actors in the process. In a [RAND report](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf), researchers emphasise how widespread AI and autonomous systems could make inadvertent escalation more likely because of “how quickly decisions may be made and actions taken if more is being done at machine, rather than human, speeds.” Two conflicting sides might equally find it necessary to use autonomous capabilities early to gain a coercive and military advantage to prevent an opponent from gaining the upper hand, raising the possibility of first-strike instability. These dynamics could have fateful consequences for how wars begin. “Because of the speed of autonomous systems having to be countered by other autonomous systems, we could find ourselves in a situation where these systems react to each other in a way that’s not predictable,” Sebastian says. ”Before you know it, a rapid escalation leads to a military conflict that wasn’t desirable in the first place.” Prakash, who is the author of [The Age of Killer Robots](https://www.amazon.com/Age-Killer-Robots-Abishur-Prakash/dp/0995833966/ref=sr_1_1?dchild=1&keywords=the+age+of+killer+robots+abishur&qid=1623803938&sr=8-1), believes governments are going to have to rethink deterrence in an era when AI is making military decisions. “Deterrence has so far revolved around stopping a nation or actor from doing something today. But as nations use technology to predict future events on the world stage – or what I call ‘[Algorithmic Foreign Policy](https://blogs.scientificamerican.com/observations/algorithmic-foreign-policy/)’ – a new challenge emerges,” he says.

### NATO Losing

#### NATO is falling behind in the AI race – standardization is needed now

Wodecki 5/4 (Ben Wodecki is Ben Wodecki is assistant editor at AIBusiness.com, “NATO at risk of losing AI innovation race to Russia, China,” AI Business, 5/4/2022, <https://aibusiness.com/document.asp?doc_id=777260>)-MP

The North Atlantic Treaty Organization (NATO) should standardize and regulate AI to keep up with rivals, according to findings published by the U.S. think tank, Center for European Policy Analysis (CEPA). CEPA’s comments came as it published a series of AI-related recommendations for NATO amid growing geopolitical tensions with the likes of Russia, China and North Korea. Its recommendations include AI standardization, encouraging and improving AI literacy and spurring private sector innovation. Such undertakings would allow NATO allies to better scale and deploy AI – and keep pace with rivals. “These new capabilities will revolutionize NATO’s military and strategic affairs, thus strengthening NATO’s ability to fulfill its essential core tasks of collective defense, crisis management and cooperative security,” CEPA’s Nicholas Nelson and Nico Luzum wrote. The pair cited AI projects being undertaken by adversaries, including China’s attempts to develop purported mind-controllable drones and AI assistants for fighter pilots. But NATO allies have their own capabilities – including U.S.-developed autonomous tanks and British-made systems that provide ground troops with information on the surrounding terrain. The think tank’s study suggests that at present, NATO is leading the AI race – but risks losing its competitive advantage to peer competitors “competitors if allies fail to leverage the private sector, coordinate implementation and engage with the public.” CEPA suggests that NATO allies should accelerate AI adoption and actively encourage private sector innovation. “Ultimately, we hope that these recommendations enable NATO allies to better innovate, scale, deploy, and integrate AI and autonomy-based technologies to form agile, system-wide solutions.

#### NATO action urgent – they need to defend their tech edge

Jankowski 21 [Dominik P. Jankowski is a security policy expert, diplomat, think-tanker and social media aficionado. Currently he serves as Head of OSCE and Eastern Security Unit at the Ministry of Foreign Affairs of the Republic of Poland. Previously he served as Chief Specialist for Crisis Management at the Ministry of Foreign Affairs (2014-2016), Expert Analyst and Head of the International Analyses Division at the National Security Bureau of the Republic of Poland (2010-2014), Senior Expert at the J5-Strategic Planning Directorate of the General Staff of the Polish Armed Forces (2009-2010) as well as foreign policy expert at the President Aleksander Kwasniewski “Amicus Europae” Foundation (2007-2010). *NATO in Era of Unpeace: Defending Against Known Unknowns.* “NATO and the Emerging and Disruptive Technologies Challenge.” Pp 96-99. March 19, 2021. Lublin Publications, https://ies.lublin.pl/wp-content/uploads/2021/03/nato-in-the-era-of-unpeace\_calosc-1.pdf#page=82]//PJ

NATO’s approach to EDTs should be based on three key objectives: Retain the technological edge Maintain the core values of the Alliance Ensure that no potential adversary gains a strategic, asymmetric advantage over NATO that could undermine the deterrence and defence posture The potential EDTs implications for NATO’s deterrence and defence remain of primary importance. Indeed, EDTs will provide a greater range of tools for adversaries to challenge and find weaknesses in NATO’s posture. At the same time, ease of commercial access to EDTs raises the prospect of new – increasingly confident – state and non-state actors to contest NATO, particularly with increased challenges of attribution. Table 2 presents an overview of the EDTs impact on NATO’s posture, including both challenges and opportunities. \*\*Table 2 omitted\*\* Moreover, based on the four broad inter-related trends presented earlier in this study, one can identify the most critical implications for NATO’s deterrence and defence. First, the maturation of the precision-strike regime appears to favour the denial of most domains relative to the ability to gain control over them. The dominant force elements of the Allied armed forces can be held at risk with precision-guided missiles for a fraction of those platforms’ costs. Yet, Allies could exploit cross-domain precision weapons to deny an opponent the ability to project power intra-regionally. By developing the “anti-access/area denial” (A2/AD) capabilities, frontline states – including on NATO’s eastern flank – could considerably strengthen NATO’s conventional deterrence. In this context, one should note that trends in precision-strike warfare call into question NATO’s preference for expeditionary defence whereby forces are dispatched reactively to reinforce frontline states. Second, disrupting an adversary’s battle network should be treated as a major warfighting mission. In doing so, the Allied armed forces will need to reduce their vulnerabilities to network attacks while improving their abilities to operate in environments where radio-frequency interference will be a likely condition. Moreover, the security of Allied military supply chains – especially with regards to semiconductor production and 5G networks – will demand greater attention as a consequence of the competition between battle networks. Finally, the struggle between opposing battle networks will hinge on the contests for control of space and cyberspace – both crucial for military surveillance, warning, battle management, and communications. Third, the contestation of space and cyberspace will require new missions for protecting assets and holding hostile systems at risk within those domains. Allies will also observe a growing use of space to deny operations in other domains. This will entail closer space cooperation between Allies in order to enhance strategic solidarity and complicate efforts by an aggressor to target the space capabilities. Fourth, the supplanting of human forces by highly autonomous machines could offer NATO a path to significantly reduce the cost of training forces to the point where they are able to achieve “first battle competence.” Autonomous systems may also offer Allies affordable means of regaining forward combat power in conflicts on the periphery of great power rivals through more distributed, swarming, and expandable forces. Table 3 offers an overview of the military implications on NATO of selected EDTs.

#### Emerging tech and threats guarantee innovation will be the make or break for NATO stability and future effectiveness.

Kallenborn 22 (Zachary Kallenborn is an author and analyst who specializes in WMD terrorism, unmanned systems, drone swarms, and homeland security. Zachary is a Policy Fellow at the Schar School of Policy and Government, a Research Affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), an officially proclaimed U.S. Army "Mad Scientist," and a Senior Consultant at ABS Group.) “Can a Focus on Innovation Save NATO?” June 23, 2022 [https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/can-focus-innovation-save-nato-203158 //](https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/can-focus-innovation-save-nato-203158%20//) ZX

NATO is rewriting its core strategic concept for the first time since 2010. As NATO bureaucrats in Brussels scribble away, NATO is beset with a plethora of security challenges. Technologies like [artificial intelligence](https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/sitting-out-artificial-intelligence) (AI) and unmanned systems raise open questions about how militaries will organize and fight in 2032. At the same time, militaries have recognized the growing dependency on known technologies in space and cyberspace. Climate change is raising the frequency and magnitude of natural hazards like hurricanes and wildfires while strengthening migration flows and general instability. China is rising in the East, using its growing economic and military might to bolster its influence in the region. And, of course, Russia has [invaded Ukraine](https://nationalinterest.org/feature/raging-toward-abyss-russia-201144). The Russian invasion of Ukraine shows clearly the inevitability of change in global security. In only a few short days after the invasion, Germany [instituted](https://nationalinterest.org/blog/buzz/germany-ramp-defense-spending-following-russian-invasion-200909) a new 100 billion euro fund to modernize its military, [Sweden and Finland](https://www.nbcnews.com/news/world/finland-nato-baltics-putin-threat-ukraine-invasion-europe-rcna17805) expressed new interest in joining NATO, and former Japanese prime minister [Shinzo Abe](https://www.bloomberg.com/news/articles/2022-02-27/japan-should-discuss-nato-like-nuclear-weapons-sharing-abe-says) called for a nuclear weapons sharing agreement. Nations throughout the world have clearly recognized the threat the Russian invasion poses to the broader international order, which is predicated on the assumption states should not invade other states. Of course, the war is not yet over, and the geopolitical dust may settle in new, unexpected ways. The NATO strategic concept should define and enhance NATO’s role as an innovation foundry. As a confederated alliance, NATO has a major strategic advantage in granting member states the freedom to innovate and diverge in how they make crucial defense and security decisions. Smaller states with fewer resources need to find more effective and efficient ways to use them. But the concepts, policies, doctrines, and strategies the smaller states develop may help inform the practices of larger member states. This allows the inherent risk of innovation to be diffused throughout the alliance. Plus, NATO dominates the world in academic excellence. In the U.S. News and World Reports' best college rankings, a non-NATO member doesn’t show up until twenty-fifth place. That college, the University of Melbourne in Australia, also happens to be located in a [close NATO partner](https://www.nytimes.com/2021/09/16/world/australia/australia-china-submarines.html). Excellent universities mean excellent research, excellent teaching, and sharper minds. That means improved technology, innovative ideas, and military leaders equipped to think critically about emerging challenges. Better applying such brilliance to defense innovation can only help the alliance take on the broad, dynamic challenges it faces. Geopolitically, Russian aggression is growing, China is on the rise, and the alliance’s future in the Middle East is uncertain. Russia has invaded Ukraine, adding another military intervention to its [list of twenty-five](https://www.rand.org/pubs/research_reports/RRA444-3.html) since 1991. Russian [active measures](https://www.nytimes.com/2021/03/16/us/politics/election-interference-russia-2020-assessment.html) also played a role in the 2016 election of former President Donald Trump, the decision for the United Kingdom to exit the European Union, and the weakening of European Union member states writ large. At the same time, Washington is quite worried about the rise of China as a competitor for global leadership and an opponent in a potential fight over an independent Taiwan. Understandably so: Chinese defense spending hit [$240 billion](https://www.sipri.org/sites/default/files/2021-01/2101_sipri_report_a_new_estimate_of_chinas_military_expenditure.pdf) in 2019 without needing to prepare for a two-front war. Chinese calls for control over Taiwan seem to have grown louder and stronger, too. The U.S. withdrawals from Iraq and Afghanistan leave NATO’s future role in the Middle East unclear. Geopolitical competition is also taking place in new domains. In the past few years, NATO has wisely identified cyberspace and space as critical domains of competition. Today’s militaries are deeply dependent on both domains. Complex computing systems support today’s advanced weapon systems and platforms, and those systems can create significant [cyber vulnerabilities](https://www.gao.gov/assets/gao-19-128.pdf). Cyberspace also allows adversaries to strike, disrupt, and even destroy critical infrastructure assets in a member state without putting a single boot on the ground. On the space front, the [Department of Defense](https://rntfnd.org/wp-content/uploads/DoD-PNT-Strategy.pdf) notes that space-based positioning, navigation, and timing are “integral to enabling the Joint Force” to carry out objectives in the National Military Strategy and National Security Strategy. Cyberspace and space are also interrelated themselves, as [satellites](https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf) depend on cyber technology. Cyber and space dependence is particularly acute when it comes to new technologies like artificial intelligence, [unmanned systems](https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/it-too-late-stop-spread-autonomous), and drone swarms. NATO has identified eight emerging disruptive [technologies](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf): big data, artificial intelligence, autonomy, quantum technologies, space technologies, hypersonics, biotechnology and human enhancement, and novel materials and manufacturing. Advancements in robotics and artificial intelligence are leading to more sophisticated unmanned systems, usable in the air, on the land, at sea, and perhaps [all of them](https://www.army.mil/article/237978/army_advances_learning_capabilities_of_drone_swarms) at once. [Quantum computing](https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/) threatens traditional encryption methods, while [quantum radar](https://asiatimes.com/2021/09/quantum-radar-does-it-actually-work/) threatens traditional stealth. Additive manufacturing allows new means of producing defense equipment, while nanotechnologies allow new types of materials with novel properties. What’s more, these technologies may interact in complex and unforeseen ways. How might artificial intelligence lead to improved bio- or nano-technologies? If quantum radar weakens the advantages of stealth, does that make cheap massed drones more valuable? Even if [these](https://www.scientificamerican.com/article/the-physics-and-hype-of-hypersonic-weapons/) [technologies](https://www.thedronegirl.com/2017/12/31/drones-overhyped/) prove to be [over-hyped](https://www.lawfareblog.com/quantum-cryptanalysis-hype-and-reality) in the short-term, technology is always growing. The evangelists may yet prove right. Three core tasks have traditionally defined NATO’s activities: collective defense, collective security, and crisis management. NATO should add a fourth: collective resilience through innovation. The aim of the new core task would be to prioritize NATO’s capacity to innovate and learn, and in so doing, bind states more tightly together as an alliance. This task would aim to expand and strengthen existing NATO efforts like the [NATO 2030 Initiative](https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf) to ensure innovation remains a key part of the alliance, not just until 2030, but until 2100. What’s more, it offers specific paths to realize the commitments NATO members made in the 2021 [Brussels Summit Communique](https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en) to strengthen NATO as an organizing framework, enhance resilience, foster technological cooperation, and strengthen NATO capacity building. The starting point for innovation is expanding research and development collaboration. NATO recently started a Defense Innovation Fund and a Defense Innovation Accelerator for the North Atlantic (DIANA). The forty-seven test centers and nine accelerators under DIANA need to be integrated as a permanent feature of the alliance as a whole, which means codifying how the accelerator sets priorities, how research results are disseminated, and how research findings support other NATO activities. NATO should also go beyond the accelerator to encourage and enable the creation of more bilateral and multilateral research agreements and general memorandums of understanding on research cooperation. But that’s just the start. NATO should launch a “War Game 2030 Initiative” to identify, experiment with, and evaluate new concepts for employing technologies and considering the ways adversaries might employ them. NATO could hold alliance-wide competitions to assess different answers to common defense questions such as: what combination of unmanned and manned systems are most effective in amphibious assault missions? Winners would earn points of military pride for their country and contribute to the alliance in ways beyond simple [defense spending](https://nationalinterest.org/feature/two-percent-defense-spending-nato-flawed-idea-27802) metrics. In addition, NATO should explore new ways to conduct war games, especially through the use of synthetic environments. NATO might partner with non-traditional stakeholders like video game designers and eSports leagues to draw on their experience in making realistic, dynamic war gaming environments. NATO has thirty members. That’s a lot of opportunities for cooperation. In fact, there are 435 possibilities for bilateral cooperation, with possibilities including everything from Albanian ties with Belgium to joint United Kingdom and American cooperation. NATO should establish a NATO diplomatic corps to help identify opportunities for interstate collaboration and support collective NATO diplomatic goals. NATO diplomats could be stationed at each NATO member state, critical non-NATO partners and rivals, and international organizations like the European Union. NATO diplomats could also help advance common NATO positions around emerging international [treaty issues](https://nationalinterest.org/feature/nuclear-ban-treaty-enters-force-posing-new-challenges-america-176865) like the Treaty for the Prohibition of Nuclear Weapons and calls to ban autonomous weapons. This would differ from existing defense attaches and inter-state diplomacy in that NATO diplomats would represent collective NATO interests, not just national interests.

### Interoperability Key

#### AI interoperability is key to maintaining effective US military alliances

**Imbrie et al. ‘20** (Andrew Imbrie, Senior Fellow at Georgetown's Center for Security and Emerging Technology; Ryan Fedasiuk, Research Analyst at Georgetown's Center for Security and Emerging Technology; Catherine Aiken, Director of Data Science and Research at Georgetown's Center for Security and Emerging Technology; Tarun Chhabra, nonresident fellow with the Center for Security, Strategy, and Technology at the Brookings Institution; Husanjot Chahal, Research Analyst at Georgetown University's Center for Security and Emerging Technology; February 2022; “HOW THE UNITED STATES AND ITS ALLIES CAN DELIVER A DEMOCRATIC WAY OF AI”; CSET; <https://cset.georgetown.edu/publication/agile-alliances/>)-amc

Interoperability is a critical lubricant for U.S. alliances. To operate effectively, allies need to plan, train, and exercise together. Joint operational concepts, com- mon 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 inter- pretability, 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 sug- gests 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.

#### Threats to interoperability now – Building AI capacity with European countries is key to prevent digital divide

Soare 20 [Simona R. Soare, Simona R. Soare 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., “DIGITAL DIVIDE? Transatlantic defence cooperation on Artificial Intelligence”, European Union Institute for Security Studies, Brief 3, March 2020, [https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%203%20AI\_0.pdf]-amc](https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%203%20AI_0.pdf%5d-amc)

There is a growing transatlantic digital gap, including on AI,21 that feeds into broader concerns around transatlantic military interoperability. Europe is already behind in the global technological competition on AI, including in R&D and technology adoption. The EU, the world’s second-largest economy, only attracts 8% of global private equity AI investment, most of which goes to the United Kingdom,22 now outside the Union. In a demonstration of the flattening effects of AI, a post-Brexit EU might attract as little AI private funding as Israel – approximately 4% of the global total. Diffusion of digital technologies in Europe remains slow and AI is mostly a niche market for European companies. The European Commission’s pledge to spend €20 billion a year for the next decade to support AI R&D, together with national European pledges, will help narrow the AI investment gap with the US and China. It may not close the gap, but it will undoubtedly make Europeans more competitive. European states are also increasing their defence spending, which means more funding will be redirected towards R&D and emerging and disruptive technologies. Nevertheless, Europe is lagging significantly behind the US and China on defence AI R&D. Of course, European defence R&D has traditionally been lower than the US and the transatlantic technology gap is an enduring feature of the relationship. At €44.5 billion, European defence investment is not negligible, but defence research is still decreasing, begging the question whether this state of affairs is sustainable. The fact that 90% of European defence AI R&D comes from 7 out of 27 countries highlights the intra-European technological divide between the AI haves and have-nots. While national AI efforts and limited bilateral cooperation may help narrow the investment and technological gaps between Washington and leading European AI champions, it will not close a structural security vulnerability for the Union and for the transatlantic partnership, with negative impact on interoperability.

### China Internal

#### AI gives China an opportunity to leap ahead in the global power race

Kania ‘19 (Elsa B Kania, Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security, “Chinese Military Innovation in the AI Revolution,” The RUSI Journal, 164:5-6, 26-34, November 29 2019, https://www.tandfonline.com/doi/abs/10.1080/03071847.2019.1693803)-amc

Chinese leaders recognise the AI revolution is a unique moment in which the PLA has the potential to leapfrog the US in terms of military power. Notably, Lieutenant General Liu Guozhi (刘国治), director of the CMC Science and Technology Commission has argued, ‘this is a rare strategic opportunity for our nation to achieve innovation surpassing and to achieve a powerful military, and it is also a rare strategic opportunity for us to achieve turning sharply to surpass (弯道 超车)’.63 In the process, the PLA will be inherently challenging – and often targeting – the US military. Indeed, the recent history of China’s military modernisation has been deeply influenced by the PLA’s concentration on the US military as both a model and a powerful potential adversary (强 敌). This approach to military science was aptly captured by an authoritative commentary in PLA Daily that urged to: Keep an eye on future opponents, adhere to using the enemy as the teacher, using the enemy as a guide, and using the enemy as a target ... We must develop technologies and tactics that can break the battle systems of powerful adversaries and counter the high- end combat platforms of powerful adversaries.64 If successful, the PLA could succeed in realising its aspirations of becoming a world-class military, changing the balance of power in the Indo-Pacific and beyond.

#### China co-op calls are lies–– DOD requests and Diverging Incentives prove

**Allen 22** (Gregory Allen, 5-20-22, Director, AI Governance Project and Senior Fellow, Strategic Technologies Program, <https://www.csis.org/analysis/one-key-challenge-diplomacy-ai-chinas-military-does-not-want-talk>) Roho

One Key Challenge for Diplomacy on AI: China’s Military Does Not Want to Talk May 20, 2022 Over the past 10 years, artificial intelligence (AI) technology has become increasingly critical to scientific breakthroughs and technology innovation across an ever-widening set of fields, and warfare is no exception. In pursuit of new sources of competitive advantage, militaries around the world are working to accelerate the integration of AI technology into their capabilities and operations. However, the rise of military AI has brought with it fears of a new AI arms race and a potential new source of unintended conflict escalation. In the May/June 2022 issue of Foreign Affairs, Michael C. Horowitz, Lauren Kahn, and Laura Resnick Samotin write: The United States, then, faces dueling risks from AI. If it moves too slowly, Washington could be overtaken by its competitors, jeopardizing national security. But if it moves too fast, it may compromise on safety and build AI systems that breed deadly accidents. Although the former is a larger risk than the latter, it is critical that the United States take safety concerns seriously. Such fears are not entirely unfounded. Machine learning, the technology paradigm at the heart of the modern AI revolution, brings with it not only opportunities for radically improved performance, but also new failure modes. When it comes to traditional software, the U.S. military has decades of institutional muscle memory related to preventing technical accidents, but building machine learning systems that are reliable enough to be trusted in safety-critical or use-of-force applications is a newer challenge. To its credit, the Department of Defense (DOD) has devoted significant resources and attention to the problem: partnering with industry to make commercial AI test and evaluation capabilities more widely available, announcing AI ethics principles and releasing new guidelines and governance processes to ensure their robust implementation, updating longstanding DOD system safety standards to pay extra attention to machine learning failure modes, and funding a host of AI reliability and trustworthiness research efforts through organizations like the Defense Advanced Research Projects Agency (DARPA). However, even if the United States were somehow to successfully eliminate the risk of AI accidents in its own military systems—a bold and incredibly challenging goal, to be sure—it still would not have solved risks to the United States from technical failures in Russian and Chinese military AI systems. What if a Chinese AI-enabled early warning system erroneously announces that U.S. forces are launching a surprise attack? The resulting Chinese strike—wrongly believed to be a counterattack—could be the opening salvo of a new war. In recognition of this risk, the National Security Commission on Artificial Intelligence recommended in its March 2021 final report that the DOD engage in diplomacy with the Chinese military to “discuss AI’s impact on crisis stability.” More recently, Ryan Fedasiuk wrote in last month’s Foreign Policy that “it is more important than ever that the United States and China take steps to mitigate existential threats posed by AI accidents.” It is not only Americans who have written about the need for a diplomatic dialogue on this subject. In 2020, Zhou Bo, a senior colonel in the People’s Liberation Army (PLA), wrote an op-ed in the New York Times in which he argued, As China’s military strength continues to grow, and it closes the gap with the United States, both sides will almost certainly need to put more rules in place, not only in areas like antipiracy or disaster relief—where the two countries already have been cooperating—but also regarding space exploration, cyberspace and artificial intelligence. Other Chinese officials—including Fu Ying, the vice chair of the China’s National People’s Congress Foreign Affairs Committee—have published similar calls for U.S.-China diplomacy on AI risk reduction. Even the Global Times, a newspaper owned and published by the Chinese Communist Party, ran an English-language article in November 2021 with the headline “China urges regulating military use of AI, first time in UN history, showing global responsibility.” Clearly China believes that calls for diplomacy on military AI are good for its global reputation. Substantive diplomacy on this topic is worth pursuing and, if successful, could meaningfully contribute to reducing the risk of a future U.S.-China conflict. With such loud public support in prominent Chinese venues, one might think that the U.S. military need only ask in order to begin a dialogue on AI risk reduction with the Chinese military. Alas, during my tenure as the Director of Strategy and Policy at the DOD Joint Artificial Intelligence Center, the DOD did just that, twice. Both times the Chinese military refused to allow the topic on the agenda. Though the fact of the DOD’s request for a dialogue and China’s refusal is unclassified—nearly everything that the United States says to China in formal channels is—the U.S. government has not yet publicly acknowledged this fact. It is time for this telling detail to come to light. China’s refusal was not the first time that China’s diplomatic strategy on military AI included a gap between words and actions. China’s 2016 and 2018 position papers to the United Nations discussions on lethal autonomous weapons have supported a ban on the usage of such weapons, but not their development. If that is the case, it begs the question why are Chinese weapons companies—including ones controlled and owned by the Chinese military— building and exporting internationally AI-enabled weapons that openly advertise lethal autonomous capabilities. And it is important that such risk reduction dialogues occur bilaterally between the DOD and the PLA, not just via the Chinese Ministry of Foreign Affairs’ public proclamations at the United Nations. The Chinese Ministry of Foreign Affairs is not a direct analogue of the U.S. State Department, which complicates its ability to authoritatively speak on behalf of the PLA. In the Chinese system, the Chinese military is a part of the Chinese Communist Party, not the Chinese government, which controls the Chinese Ministry of Foreign Affairs. Though both organizations ultimately have the same leader—Xi Jinping is both the president of the People’s Republic of China and chairman of the Chinese Communist Party—experience has shown that there is no substitute for direct DOD-PLA dialogue on military issues. It is frustrating that China’s public calls for diplomatic dialogue and the cooperative development of new norms on military AI—which have continued even after the PLA’s multiple refusals to have such a dialogue—have attracted praise from those who are evidently not aware of the gap between public rhetoric and private reality. For example, Michael Woolridge, an AI researcher at Oxford University, highlighted China’s public diplomacy on military AI in his recent book as encouraging evidence that China was seriously considering the concerns being raised by both AI researchers and Chinese international relations scholars. The truth, unfortunately, is that—despite the United States’ efforts at transparency and requests for dialogue—the United States knows very little about how seriously the Chinese military considers ethics in its use of AI, how robust Chinese test and evaluation processes are, and what governance structures and procedures exist to reduce the risk of military AI accidents.That secrecy in and of itself is a source of risk to international peace and security. But, then again, what incentive does China have to substantively engage? The United States is already providing a great deal of transparency around its own risk reduction efforts, and China is already garnering many reputational benefits from calling for dialogue without any of the costs of substantively participating. Perhaps neither the U.S. government nor the Chinese scholarly community can succeed in persuading the PLA that it is in everyone’s best interest for this dialogue to occur. At the very least, however, it should be clear to the international community that China is the one refusing to talk.

#### DOD needs allies to stay on top

**Ryseff 20** (JAMES RYSEFF, 10-9-20, technical policy analyst at the nonprofit, nonpartisan RAND Corporation., <https://warontherocks.com/2020/10/the-united-states-can-only-achieve-ai-dominance-with-its-allies/>) RoHo

As the United States races with China to apply artificial intelligence for military purposes, many experts worry that it may be hampered by a shift in the nature of AI. The conventional wisdom has been that, until now, American technologists could depend on elite researchers and faster computers to outperform their Chinese rivals. However, these advantages are no longer the keys to harnessing AI most effectively. Data is. Chinese AI experts believe that China’s larger population and lax privacy controls give China a durable advantage in collecting the best data sets to teach AI algorithms how to optimize their performance. Kai-Fu Lee, China’s most prominent AI researcher, has dubbed China the “Saudi Arabia of data” and argues that China’s data advantage is expanding by the day. The Center for Data Innovation, an American think tank, agrees, calculating that the Chinese population generates terabytes more information than Americans do. In reality, determining who holds the advantage in data is far more complicated than simply counting how many bytes of information are stored in each country. As a recent Center for Security and Emerging Technology report rightly points out, the quality of data and how well it has been curated and labeled usually matter more than simply how much data one has. Even so, the analysts take for granted that China’s size will ultimately give it the advantage in commercial data, one that may let its corporations overtake their American counterparts in AI. However, these conclusions overlook the primary advantage American technology companies hold over their Chinese counterparts: its global user base. For companies like Google and Facebook, the competition to amass data is not between the digital activities of 330 million Americans against the virtual footprint of over one billion Chinese citizens. Instead, their products hold near-monopolies in the United States, Europe, Latin America, Africa, and most of Asia. In contrast, Chinese equivalents like Baidu and WeChat have only a handful of non-Chinese users. This global reach gives American technology companies an advantage both in the total volume of data they collect and in the diversity of data harvested. Chinese data sets, for now, are still largely blind to conditions outside of China. AI algorithms trained on those data sets would struggle to travel outside its borders. The success of American technology companies illustrates the most promising path for the U.S. military to pursue at the dawn of its own AI age. That does not mean that the Department of Defense should simply copy Silicon Valley’s strategy mindlessly. While data from the commercial sector — such as an individual’s social connections, current employer, or personal finances — will continue to be a gold mine for global intelligence agencies, data relevant to the future battlefield will primarily concern soldiers, vehicles, training exercises, and the like. No organization will have more relevant data for these use cases than the military itself. Fortunately, the Defense Department has positioned itself well to become the globally dominant platform for military data, just as American technology companies dominate the global marketplace in their realms. The United States counts most industrialized nations as military allies and equipment manufactured by the United States or its NATO allies is driven and flown around the world. However, the Defense Department has yet to capitalize on this potential. NATO weapons and vehicles were originally designed to be interoperable in an industrial-age sense, shooting the same bullets or refueling from the same connectors. Unfortunately, NATO has not yet upgraded for the information age. The data generated by U.S. Army tanks cannot easily be accessed or aggregated with data generated by Marine Corps tanks, let alone British ones. Just as the Goldwater-Nichols Act once pushed America’s separate armed services to break out of their isolated battlefield domains, military data must now discover how to operate jointly as well. Three initiatives could be critical to accomplishing this. First, the Defense Department could create a 10-year roadmap for upgrading data interoperability that lays out specific operational objectives to demonstrate improvements. To ensure these objectives are met, they could be incorporated into the major annual exercises conducted with NATO and East Asian allies. For example, American and South Korean units could draw spare parts and other consumables from each other during their annual training exercises. Throughout the exercise, both sides could confirm their logistics databases can combine to present a unified picture of the allied logistical situation and provide projections of future needs as the simulated combat event evolves. Establishing tangible objectives and aligning the timeframe with existing multinational exercises will be the key to success. Militaries invest a great deal of time and effort training their personnel to be ready for the fight. They must now learn how to “train” and prepare their data as well. This can mean many things. When training their personnel, militaries spend some of their time imparting specific skillsets that will be useful in combat. In other cases, soldiers learn how to work together to solve unforeseeable problems as they arise — or simply learn how the operational routines of other units or allied militaries differ from their own. Regardless, commanders recognize their soldiers must routinely practice their skills under real-world conditions if they will be expected to work as an effective team on the battlefield. Data needs the same types of preparation to be ready for its role in the fight. Much as soldiers need to leave the garrison and work through practical exercises in the field, it is not enough to develop a technical specification documenting how two data sets are supposed to work together. Someone needs to actually make the data sets work together. They must be routinely explored, analyzed, and aggregated to solve real problems in order to ensure they will remain interoperable and effective. Similarly, the analysts and engineers responsible for curating data need opportunities to interact with each other in order to develop the operational routines necessary to ensure effective collaboration during a crisis. Without these forcing functions, too much military data will remain isolated and unusable at the scale needed to engineer AI algorithms. Second, the military may need to collaborate with allies to achieve common understandings about when and how to share data. European governments in particular have begun to codify digital norms for the consumer space in frameworks like the General Data Protection Regulation and the establishment of new legal concepts like the Right to be Forgotten. The United States could play a role in shaping the equivalent norms in the national security and public policy space. Otherwise, fragmented data repositories from the United States and its allies may not be able to achieve the critical mass — that is, gather enough data — necessary to compete with China’s data warehouses. Past disagreements between the United States and its allies over norms related to atomic weapons demonstrate how these considerations can ultimately impact military operations. In Europe, the United States managed to forge an agreement that allowed the stationing of tactical nuclear weapons on the territory of its NATO allies, even in the face of significant domestic opposition in key nations such as West Germany. In contrast, the United States was unable to achieve a similar consensus among its allies in Asia. Both Japan and New Zealand banned the introduction of nuclear weapons into their territory, causing headaches for U.S. Navy operations in the region. While in that case Navy ships could find alternate ports to operate from, a similar divergence in norms would have much greater consequences for the U.S. military’s ability to develop AI. Data withheld is data lost. Most norms about the use of military data will likely be uncontroversial. Unlike Facebook or Google, whose business models depend on precisely targeting ads at their user bases, militaries in democracies have little reason to exchange personally identifiable information or other sensitive details about their citizens. Norms about controversial topics such as autonomous systems may prove more difficult to forge a consensus around. Agreements that data provided by partners would not be used to train these systems without explicit consent could be a compromise acceptable to all parties. Finally, the United States could seek deeper integration and cooperation with its allies who have unique resources to advance specific applications of AI. Many, including the National Security Commission on Artificial Intelligence, have called for the United States to leverage its existing “Five Eyes” alliance and extend it to include cooperation in AI. A complementary approach might be to focus on partners who have unique technical assets to contribute. For example, East Asian allies such as Japan and South Korea have invested heavily in robotics and automation, which makes them attractive partners for developing more capable drones and other autonomous vehicles. They may also have fewer hesitations about deploying these technologies than other potential partners. Similarly, the Israeli government has carefully incubated a world-class cyber security sector, potentially positioning it as a valuable collaborator in training AI-enhanced cyber defenders how to protect critical infrastructure and assets. Ultimately, close collaborators in any AI alliance must pass two tests: They must be able to usefully contribute to the work, and they will also need to be trustworthy enough to share in these cutting-edge technical advancements. While achieving the kind of close collaboration with allies that the United States has enjoyed in other realms may be difficult, it will be essential if the United States hopes to achieve the data dominance needed to succeed in future combat.

#### AI dev is in China’s hands which is wildly dangerous – The US is falling behind

**Allison ‘20** (Graham Allison, Douglas Dillon Professor of Government, Harvard Kennedy School Member of the Board, Belfer Center Former Director, Belfer Center Faculty Affiliate, Future of Diplomacy Project,August 2020, <https://www.belfercenter.org/publication/china-beating-us-ai-supremacy>)Roho

The US-China Race for Artificial Intelligence Combining decades of experience advancing frontier technologies, on the one hand, and analyzing national security decisionmaking, on the other, we have been collaborating over the past year in an effort to understand the national security implications of China’s great leap forward in artificial intelligence (AI). Our purpose in this essay is to sound an alarm over China’s rapid progress and the current prospect of it overtaking the United States in applying AI in the decade ahead; to explain why AI is for the autocracy led by the Chinese Communist Party (hereafter, the “Party”) an existential priority; to identify key unanswered questions about the dangers of an unconstrained AI arms race between the two digital superpowers; and to point to the reasons why we believe that this is a race the United States can and must win. We begin with four key points. First, most Americans believe that U.S. leadership in advanced technologies is so entrenched that it is unassailable. Likewise, many in the American national security community insist that in the AI arena China can never be more than a “near-peer competitor.” Both are wrong. In fact, China stands today as a full-spectrum peer competitor of the United States in commercial and national security applications of AI. Beijing is not just trying to master AI—it is succeeding. Because AI will have as transformative an impact on commerce and national security over the next two decades as semiconductors, computers and the web have had over the past quarter century, this should be recognized as a matter of grave national concern.1,2,3 Second, China’s zeal to master AI goes far beyond its recognition that this suite of technologies promises to be the biggest driver of economic advances in the next quarter century. For the Party, AI is mission critical. The command of 1.4 billion citizens by a Party-controlled authoritarian government is a herculean challenge. Since the fall of the Soviet Union, Americans have been confident that authoritarian governments are doomed to fail—eventually. But AI offers a realistic possibility of upending this proposition. AI could give the Party not just an escape hatch from the “end of history,”4 but a claim to advance a model of governance—a national operating system—superior to today’s dysfunctional democracies. As one former Democratic presidential candidate put it: “China is using technology to perfect dictatorship.”5 It’s a value proposition that resonates with many leaders around the world. As former Google ceo Eric Schmidt has argued: “if the Soviet Union had been able to leverage the kind of sophisticated data observation, collection and analytics employed by the leaders of Amazon today, it might well have won the Cold War.” Third, while we share the general enthusiasm about AI’s potential to make huge improvements in human wellbeing, the development of machines with intelligence vastly superior to humans will pose special, perhaps even unique risks. In 1946, Albert Einstein warned, “the unleashed power of the atom has changed everything save our modes of thinking, and thus we drift towards unparalleled catastrophe.” We believe the same could be said of AI. Henry Kissinger has identified these risks in what we call “Kissinger’s Specter.” In his words, AI threatens an unpredictable revolution in our consciousness and our thinking, and an “inevitable evolution in our understanding of truth and reality.”6 In response to Einstein’s insight, the technologists and strategists who had built and used the bomb to end World War II joined forces to find ways to prevent a nuclear World War III. Meeting the challenges posed by AI will require nothing less. Fourth, China’s advantages in size, data collection and national determination have allowed it over the past decade to close the gap with American leaders of this industry. It is currently on a trajectory to overtake the United States in the decade ahead. Nonetheless, if the United States will awake to the challenge and mobilize a national effort, we believe that it can develop and execute a winning strategy. For many readers, AI is just the latest bright, shiny object on the technology horizon. A brief explainer to provide some further context may be helpful. AI encompasses big data, machine learning and multiple related technologies that allow machines to act in ways humans describe as “intelligent” when we do the same thing.7 For example, consider gps navigation app Waze locating the best route through heavy traffic; Amazon’s eerily relevant product suggestions; or the programmed machines that now regularly defeat world masters in chess. Today’s leading information technology companies—including the faangs (Facebook, Amazon, Apple, Netflix and Google) and bats (Baidu, Alibaba and Tencent)—are betting their r&d budgets on the AI revolution. As Amazon’s Jeff Bezos said this year, “We’re at the beginning of a golden age of AI.”8

#### China is winning the AI war– Chinese investment and schooling massively increased

**Allison ‘20** (Graham Allison, Douglas Dillon Professor of Government, Harvard Kennedy School Member of the Board, Belfer Center Former Director, Belfer Center Faculty Affiliate, Future of Diplomacy Project,August 2020, <https://www.belfercenter.org/publication/china-beating-us-ai-supremacy>) Roho

China’s AI Surge Though still in their infancy, AI technologies will be drivers of future economic growth and national security. From facial recognition and fintech to drones and 5g, China is not just catching up. In many cases, it has already overtaken the United States to become the world’s undisputed No. 1. In some arenas, because of constitutional constraints and different values, the United States willfully forfeits the race. In others, China is simply more determined to win. China’s AI surge is so recent that anyone not watching closely has likely missed it. As late as 2015, when assessing its international competition, American industry leaders—Google, Microsoft, Facebook and Amazon—saw Chinese companies in their rearview mirrors alongside German or French firms in the third tier. But this changed four years ago—in 2016—when leading AI application company DeepMind fielded a machine that defeated world champion Lee Sedol in the world’s most complex board game, Go.9 Even after several American companies’ machines had bested the chess masters of the universe10, most Chinese remained confident that machines could never beat Go champions, since Go is ten thousand times more complex than chess. Thus, DeepMind’s decisive victory became for China a “Sputnik moment”11—a jolt as dramatic as the Soviet Union’s launch of the first satellite into space that sparked America’s whole-of nation surge in math and science, nasa’s creation and the original “moon shot.” Kai-Fu Lee’s book AI Superpowers offers an insightful summary of China’s engagement in the field. It began with President Xi Jinping’s personal reaction to the defeat of the world’s Go champion. Declaring that this was a technology in which China had to lead, he set specific targets for 2020 and 2025 that put China on a path to dominance over AI technology and related applications by 2030.12 Recognizing that this would have to be led by entrepreneurial companies rather than agencies of government, he designated five companies to become China’s national champions: Baidu, Alibaba, Tencent, iFlytek and SenseTime.13 Twelve months after Xi’s directive, investments in Chinese AI startups had topped investments in American AI startups.14 By 2018, China filed 2.5 times more patents in AI technologies than the United States.15 And this year China is graduating three times as many computer scientists as the United States. In contrast to nuclear weapons—where governments led in discovery, development and deployment—AI and related technologies have been created and are being advanced by private firms and university researchers. The military establishments in Washington and Beijing are essentially playing catch-up, adopting and adapting private-sector products. Where do these two competitors stand in the AI race today? Consider leading indicators under six key headings: product market tests, financial market tests, research publications and patents, results in international competitions, talent and national operating environments. Consumers’ choices of products in markets speak for themselves. In fintech, China stands alone. Tencent’s WeChat Pay has nine hundred million Chinese users,16 while Apple Pay only has 22 million in the United States.17 And when it comes to capability, WeChat Pay can do much more than Apple Pay. Chinese consumers use their app to buy coffee at Starbucks and new products from Alibaba, pay bills, transfer money, take out loans, make investments, donate to charity and manage their bank accounts. In doing so, they generate a treasure trove of granular data about individual consumer behavior that AI systems use to make better assessments of individuals’ credit-worthiness, interest in products, capacity to pay for them and other behavior. In mobile payments, Chinese spend $50 for every dollar Americans spend, in total, $19 trillion in 2018.18 U.S. mobile payments have yet to reach $1 trillion. Credit cards are as old-fashioned to Chinese millennials as handwritten checks are to their American counterparts. Mark Zuckerberg has noticed: Facebook’s major moves last year into digital payments,19 including the recent introduction of Facebook Pay, are copying Tencent, rather than the other way around. In facial recognition, the world’s most valuable AI startup is Chinese company SenseTime20—a company whose headquarters Graham visited in October. (While there, Graham also took a tour of Zhongguancun—China’s version of Silicon Valley—guided by Kai-Fu Lee whose hedge fund is one of the leading VC investors in Chinese AI startups.) In 2018’s international competition for facial recognition, Chinese teams claimed the top five places.21 Chinese firms—such as Hikvision and Dahua Technology, which control a third of the world’s security camera market22; Tiandy, whose cameras need light from only a single star at night to capture high-definition color images23; and Wuhan Guide Infared, which specializes in infrared and thermal imaging—are working hand in glove with their government to perfect facial recognition for profit and control. In this domain, there is no U.S.-China contest; the United States has essentially conceded the race because of concerns over the average individual’s privacy, and deep reservations about how this technology could be deployed. Westerners were alarmed in 2017 when researchers at Stanford created an AI algorithm that could detect with shocking accuracy individuals’ sexual orientation simply by scanning a single photo24. It does not take much imagination to consider how less socially liberal governments would apply this technology. So while San Francisco recently banned facial recognition technologies, the Party has given China’s top four facial recognition firms access to its database of over 1.4 billion citizen photos. One well-informed venture capitalist in this arena estimates that Chinese facial recognition firms have 1 million times more images than their U.S. counterparts. In speech tech, Chinese are beating American firms in all languages—including English. The world’s top voice recognition startup is China’s iFlytek. Its user base is seven hundred million, almost twice the 375 million people who speak to Apple’s Siri.25 In system performance competitions, iFlytek regularly beats teams from Google, Microsoft, Facebook, ibm and mit, all in its second language.26 At Stanford’s international challenge for machine reading comprehension, Chinese teams won three of the top five spots, including first place. Baidu developed a human-level speech recognition system a year before Microsoft did. Who was the U.S. Army’s major supplier of commercial drones until 2017—when the United States prohibited purchases for foreign suppliers?27 Shenzhen drone maker DJI, which controls 70 percent of the global market28. Drones would be just miniature hobby helicopters without elementary AI, which gives them computer vision for targeting weeds or weapons, and enables them to operate in swarms. As the recent attack on Saudi Arabia’s principal oil facilities demonstrated, the world has just begun to discover the security consequences of AI-enhanced drones operating literally below the radar. Of the world’s top five commercial drones brands, 3 are Chinese; 1 American.29 5g infrastructure will be the backbone that enables AI to reach further into everyday life, from automated cars to smart glasses. China’s Huawei is the world’s leading supplier of this telecom equipment. Not only does it own the Chinese market, which will be the world’s largest, but its 28 percent global market share nearly equals the combined shares of its two top competitors.30 Of the top four brands that will build 5g infrastructure, two are Chinese and zero are American. Chinese firms own twice as many 5g -essential patents as American firms. While the outcome of the current U.S. government campaign against Huawei remains uncertain, the company is currently delivering 5g systems well ahead of all competitors and is bringing a 5g phone to market a year ahead of Apple, the company that invented the iPhone. Financial markets reflect these realities. Five years ago, two of the world’s twenty most valuable internet companies were Chinese; today, nine are. The “Seven Giants of the AI age”—Google, Amazon, Facebook, Microsoft, Baidu, Alibaba and Tencent—are split on either side of the Pacific. Of every ten venture capital dollars invested in AI in 2018, five went to Chinese startups; four to American firms.31 Of the world’s top ten AI startups, half are American and half are Chinese. Chinese investments in AI research and development have surged to American levels, and the results are beginning to show it. The blunt truth is that China is laying the intellectual groundwork for a generational advantage in AI. According to the Allen Institute for Artificial Intelligence’s authoritative assessment, China would overtake the United States in 2019 in the most-cited 50 percent of AI papers. It will take the lead in the most-cited 10 percent this year. And by 2025, the United States will fall to second in the top 1 percent of papers.32 (Fortunately, in breakthrough papers, China remains behind.) In public patents for AI technologies, China passed the United States in 2015, and in 2018 filed 2.5 times more than America.33 In machine learning’s hottest subfield—deep learning—China has six times more patent publications than the United States. (Raw numbers, however, must be taken with a grain of salt, since not all patents are equal.) China is investing heavily in the necessary hardware as well. In 2001, China had none of the world’s five hundred fastest supercomputers. Last year, it had 219 (the United States has 116).34And while China’s supercomputers previously relied on American semiconductors, its top machine today was built entirely with domestically-manufactured processors. Like Olympic athletes, AI researchers are eager to demonstrate their progress and prowess in international competitions. As mentioned earlier, in 2017, DeepMind’s AlphaGo Master defeated the Go world’s top champion Lee Sedol a decade sooner than experts had predicted. Eight months later, Tencent’s own Go program, called “Fine Art,” also beat Sedol. And Fine Art won despite giving Sedol a two-turn head start—a handicap DeepMind has been unwilling to offer.35 Meanwhile, at the International Aerial Robotics Competition, the world’s longest-running university robotics competition, the top three performers last year were all Chinese entries.36 And in the world’s most prestigious computer science competition for secondary school students, the International Olympiad in Informatics, Chinese have won eighty-four gold medals while Americans have won fifty-two. Achieving this success in competitions reflects the investment China has made in cultivating talent. In AI, brain power matters more than computing power. China annually graduates four times as many stem students than the United States (1.3 million vs. 300,000) and three times as many computer scientists (185,000 vs. 65,000). In the U.S. News & World Report ranks, China’s Tsinghua University is number one in the world in computer science. Of every ten computer science Ph.Ds graduating in the United States today, three are American and two are Chinese. Three decades ago, only one of every twenty Chinese students studying abroad returned home. Now, four of every five do.37

#### China has numerous advantages over the US in AI

**Allison ‘20** (Graham Allison, Douglas Dillon Professor of Government, Harvard Kennedy School Member of the Board, Belfer Center Former Director, Belfer Center Faculty Affiliate, Future of Diplomacy Project,August 2020, <https://www.belfercenter.org/publication/china-beating-us-ai-supremacy>)Roho

Drivers of Competititon Culturally, many Chinese embrace what many Americans see as a nightmare “surveillance state.” Even for applications that will clearly improve public health and safety, Americans are evenly split between those who are “very willing” and those who are “very unwilling” to share personal data. In China, the willing outnumber the unwilling five to one.38 As an American-educated Chinese colleague observed, Chinese are as puzzled by Americans’ acceptance of monthly mass shootings as much as Americans are puzzled by Chinese acceptance of a government surveillance that keeps them and their families safe from such horrors. China’s government, laws and regulations, public attitudes about privacy, and thick cooperation between companies and their government are all green lights for its advance of AI. In the United States and Europe, yellow and red lights abound. President Donald Trump’s statements about AI have essentially been rhetorical. In contrast, China’s president gets it. AI is a central pillar in his agenda to “make China great again.” In a process that reminds careful observers of the leadership of Amazon and Google, he has defined key performance indicators for its development, provided massive funding for specific projects, and done whatever possible to create favorable tailwinds. Wherever the Chinese government can protect companies (in its domestic market), support national champions (through subsidies and access to government data) and enable corporations leading AI charge, it does. It is ambitious performance targets that incentivize China’s fifteen cities with populations of more than 10 million and one hundred cities with populations of more than 1 million to compete in deploying sensors in highway systems (that will support driverless cars), cameras in the “sharp eyes” program that surveil public and private properties, and an array of similar collection technologies that create “smart cities.” On each of these fronts, there are, of course, competing considerations. A more comprehensive net assessment would require drilling down at length in each area of competition. On the current path, we expect that, for the next decade, the United States will maintain its lead in enterprise software (e.g. business tools like automatic billing), advanced semiconductors and quantum computing. Nonetheless, assessing the rivalry in the decade ahead, we believe that the United States and China must be recognized as peer competitors. U.S. advantages include its position as first mover (that has allowed Facebook and Google to lead not just in American domestic markets but worldwide); the current cadre of superstars pushing the frontier of research; the ability and determination of Silicon Valley to recruit the 0.0001 percent most capable individuals from 7.7 billion people around the globe; and an ecosystem that actively encourages disruptive invention and innovation. At the same time, American AI faces serious headwinds, including a culture that values privacy over security, distrusts authority and is suspicious of government; it companies wary of working with the U.S. Defense Department and intelligence agencies; dysfunctional public policies inhibiting recruitment and immigration; laws that make it difficult to compile big data sets; and the prospect of further regulations and antitrust action against the companies that are now America’s national champions—and are driving American advances in this arena. In the longer-term competition, China’s advantages begin with its population of 1.4 billion that creates an unparalleled pool of data and talent, the largest domestic market in the world, and information collected by companies and government in a culture that values security over privacy. Its commitment to education creates an army of less expensive labor willing and able to spend substantial amounts of time cleaning data sets. Its universities are graduating computer scientists in multiples of their American counterparts, all of them eager to develop algorithms to solve social problems. Because a primary asset in applying AI is the quantity of quality data, China has emerged as the Saudi Arabia of the twenty-first century’s most valuable commodity.39 The total data created, captured and copied in China is already far greater than in the United States. In addition, the country has hungry entrepreneurs like Alibaba’s Jack Ma and Tencent’s Pony Ma; a government that is leading a whole-of-nation campaign to become the world’s leader in AI; and a national sense that China’s time has come. To the extent that the next decade is an era of implementation, the advantage lies with China. In implementation, the overwhelming competitive advantage is quantity of quality data. Both in collection and in having a cadre of grunts to clean the data, China wins. In contrast, though, if the most significant advances in AI in the next decade come from breakthrough leaps, like the development of deep learning, the advantage lies with the United States.40 Both the fact that half the world’s AI superstars work for American companies and that the United States can recruit from all the world’s people—while inherent insularity restricts China to its own population—provide advantages Beijing cannot match.

### Russia Internal

#### Russia developing AI to challenge NATO – they will engage in new security cooperation and disruptive strategies

Jankowski 21 [Dominik P. Jankowski is a security policy expert, diplomat, think-tanker and social media aficionado. Currently he serves as Head of OSCE and Eastern Security Unit at the Ministry of Foreign Affairs of the Republic of Poland. Previously he served as Chief Specialist for Crisis Management at the Ministry of Foreign Affairs (2014-2016), Expert Analyst and Head of the International Analyses Division at the National Security Bureau of the Republic of Poland (2010-2014), Senior Expert at the J5-Strategic Planning Directorate of the General Staff of the Polish Armed Forces (2009-2010) as well as foreign policy expert at the President Aleksander Kwasniewski “Amicus Europae” Foundation (2007-2010). *NATO in era of Unpeace: Defending Against Known Unknowns.* “NATO and the Emerging and Disruptive Technologies Challenge.” Pp 90-96. March 19, 2021. Lublin Publications, https://ies.lublin.pl/wp-content/uploads/2021/03/nato-in-the-era-of-unpeace\_calosc-1.pdf#page=82]//PJ

Russian EDTs Development Russia has been closely monitoring the United States as well as China’s technological priority areas while evaluating their long-term consequences and searching for means to counter them. According to Michael Raska, the current Russian EDTs strategy has been based on two elements. First, the strategy must counter the third offset strategy with the first offset strategy, which means prioritizing the development of a wide array of both strategic and tactical nuclear weapons systems: “In Russian strategic thought, maintaining a variety of sophisticated nuclear weapons can invalidate any conventional advantages of the United States, NATO, and China. Ensuring that Russia remains a nuclear superpower is the basis of all Russian security policies. Moscow has never ceased the development of strategic and tactical weapon systems even during the darkest days of 1990s, and indeed accelerated research and development during the period of swift economic growth in the 2000s.”15 Indeed, for Russia nuclear weapons are the most cost-effective pillar of strategic deterrence. Second, Russia began to counter numerous U.S. and Chinese technological initiatives using similar indigenous programs, although more narrowly focused and smaller in scale. In October 2012, Russia established the Advanced Research Foundation (ARF).16 As emphasized by Michael Raska, “the ARF focuses on R&D of high-risk, high-pay-off technologies in areas that include hypersonic vehicles, artificial intelligence, additive technologies, unmanned underwater vehicles, cognitive technologies, directed energy weapons, and others. While Russian technologies are at the early stages in some areas, in key areas such as directed energy weapons, rail gun, hypersonic vehicles, and unmanned underwater vehicles, programs are progressing into advanced stages, backed by considerable financing for many years prior to the ARF.”17 However, the challenge for Russia remains sustained resource allocation to transform these disruptive technologies into actual military capabilities. Due to its current relationship with the West, one should expect that Russia will try to establish new industrial partnerships with major non-Western countries, primarily India and China. The goal of the potential cooperation will be to secure financing and technological cooperation on these projects. In fact, “Russia has already had a positive experience with India (BrahMos cruise missile joint production venture), and has embarked on two major joint programs with the Chinese – a wide-body passenger aircraft and advanced heavy helicopter programs. The interest in establishing the new joint programs with the Chinese is especially strong in the Russian space industry. The purchase of Chinese space-grade microchip production technology in exchange for RD-180 liquid-fuel rocket engine technology is under negotiation and may start a new stage in Sino-Russian cooperation.”18 The results of the Russian Science and Technology Foresight – a full-fledged study targeted at the identification of the most promising areas of science and technology development in Russia as it nears 2030 – revealed that in numerous areas Russia is lagging behind the world leaders. Foresight 2030 covered seven priority areas: Information and communication technologies Biotechnology Medicine and health New material and nanotechnologies Rational use of nature Transportation and space systems Energy efficiency and energy saving19 In information and communication technologies, Russia occupies advanced positions in areas like “New data transfer, networking, and content distribution technologies.” However, it lags behind global leaders in most fields, in particular “Computer-aided element base design technologies” or “New data transfer technologies.”20 With regard to biotechnology, the most advanced areas of applied research in Russia identified in the study include “High-performance techniques for genome, transcriptome, proteome, and metabolome analysis,” as well as “Systematic and structural biology.”21 When it comes to medicine and health, Russia has as yet made only modest progress in human organs regeneration. Nevertheless, according to Gokhberg, et al., Russia’s best chances to achieve sound practical results are in such fields as “Biocompatible biopolymeric materials” and “Techniques for fast identification of toxic substances and pathogens.”22 Unlike most of the other priority areas, the level of research and development in new material and nanotechnology in Russia is assessed as high, particularly in such fields as “Nano-size catalysts for deep processing of raw materials” and “Nano-structured membrane materials.”23 Finally, in transportation and space systems, the research and development fields with the highest domestic competitive advantage include “Development of research models to study transport situation in the Arctic and subarctic areas” and “Development of air- and spacecraft to launch suborbital small-size space satellites.”24 At the same time, Russia is speeding up its work on artificial intelligence. President Vladimir Putin has said on numerous occasions that the leader in the field of AI would become “the master of the world.” In October 2019, Russia adopted a National Strategy for the Development of Artificial Intelligence Through 2030. According to Elena Chernenko and Nikolai Markotkin, Sberbank president German Gref was the driving force behind the strategy, and the stateowned bank prepared a roadmap for developing AI in Russia.25 In November 2019, the internet giants Yandex and Mail.ru Group, along with Gazprom Neft energy company, MTS, and the Russian Direct Investment Fund, formed a structure known as the AI Russia Alliance which is tasked with promoting Russia’s AI-based technologies. The alliance is expected to coordinate the efforts of the business and scientific communities to achieve the objectives set forth in the national AI strategy. Therefore, as Elena Chernenko and Nikolai Markotkin emphasize, in the near future the driving force behind Russian AI technologies will be commercial investment, with large IT companies – rather than start-ups – being in the driver’s seat. Still, the military sector is one of the strongest in terms of developing Russian AI. Increasingly, Russian military specialists in the field of AI applications are making advances in the use of such technologies, primarily in the maritime context. As Roger McDermott underscores, “Moscow’s interests in the use of AI to further develop maritime military capabilities relates to the future development of surface and sub-surface platforms that will be fully roboticized. Alongside this longer-term ambition is the use of situational analysis technology to ensure that naval commanders gain an advantage in time and space over a potential adversary by using the AI system to foresee the development of any situation within an operational environment, thus helping to gain the initiative. However, this is taking place within a much wider context of Moscow’s increasingly proactive interest in using AI technologies, which is changing the face of its conventional military capability and will do so for years to come.”26 The extent to which Moscow has prioritized, developed, and continued to plan future advances in applying AI within the military has to a large degree been underestimated by the West. With the introduction of AI in the fields of maritime security, engine production, or in enhancing command and control, there is no doubt that AI is finding expanding roles in the Russian Armed Forces. In this context, one should stress that Russia is a technologically advanced country in the design and development of armaments, even if its manufacturing and budgetary capacity has seldom matched its strategic ambition. Indeed, it is important not to underestimate the strength and resilience of Russia’s scientific community and innovation potential. Russian advantage is its ability to match technology with the applicable operational concepts and force and command structures. In fact, Russia has been able to use both symmetrical and asymmetrical means and methods of warfare. As Katarzyna Zysk emphasizes, “the objective has been to undermine or circumvent the opponent’s military-technological superiority and exploit its vulnerabilities, preferably in a cost-effective manner politically and economically.”27 Therefore, disruptive technologies should not be seen in isolation from disruptive strategies. In fact, technologies enable strategies. With Russia, one needs to consider not only advances in high technology for traditional military applications, but also innovations and uses below the level of declared war. Russia’s premier disruptive strategy is intimidation – to instill the awe and terror of war in adversaries in order to weaken and fracture them, all while using technology as an enabler. In peacetime, they intimidate opponents through various psychological methods, from disinformation to targeted nuclear exercises. In wartime, they use surprise and deception and are prepared to undertake asymmetric operations to destabilize, overwhelm, and fracture the adversary. Indeed, Philip Breedlove and Margaret E. Kosal insist that “understanding Russian approaches to technology development would not be complete without acknowledging the role that dezinformatsiya, disinformation, and maskirovka, military deception, play in interactions with external actors.”28

#### Russia’s trying to jump ahead in technological warfare

[Zysk](https://www.tandfonline.com/author/Zysk%2C+Katarzyna) ’20 (Katarzyna Zysk; Katarzyna Zysk is a professor of international relations and contemporary history at the Norwegian Institute for Defence Studies (IFS), which is part of the Norwegian Defence University College (NDUC) in Oslo; “Defence innovation and the 4th industrial revolution in Russia,” Taylor Francis Online, December 8 2020; <https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090?cookieSet=1>)-amc

The Russian General Staff attaches critical importance to winning and holding information superiority and influencing the cognitive-psychological domain, seen as key in any contemporary conflict. Influence operations and other forms of AI-enabled and AI-augmented ‘information confrontation’ (informatsionnoe protivoborstvo)[118](https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090) exploiting new forms and roles of information and social interaction are set to play an increasingly prominent role in Russia’s military strategy.[119](https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090) Sergei Chvarkov, professor at the Russian Academy of Military Sciences, points that cyber weapons have several critical advantages and in some cases may be many times more effective than physical destruction by conventional weapons; moreover, threats and attacks in the information sphere are hard to retaliate against.[120](https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090) The exploitation of big data is likely to play a significant role in enhancing existing and creating new means of confrontation. It requires creating an infrastructure and conditions for big data harvesting, considered by the Russian authorities? a key factor in AI development. To this end, the Russian national AI strategy clearly states that priority in accessing big data will be given to state actors.[121](https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090) Russia has also demonstrated interest in combining new technologies, such as AI and drones, in order to augment traditional methods of influence operations such as disinformation, demoralisation and propaganda. Specially developed Russian drones and cell site simulators have been able to impersonate cell phone towers with the objective of intercepting, jamming, spoofing or broadcasting tailored content on civilian mobile phones belonging to the opposing side. Russia has tested such systems in operations in Eastern Ukraine and Syria by delivering content to cell phones of opposing fighters. Based on information harvested from the smartphones, the projected content was intended to harass, intimidate and undermine morale, for instance by revealing seemingly compromising details about the adversary’s commanders or divulging knowledge about soldiers’ own families. Such methods have also been used against NATO soldiers deployed in the Baltic republics as a part of NATO’s Enhanced Forward Presence, apparently for similar influence operation purposes.[122](https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090) Furthermore, Russia has been investing in counter-network capabilities that could disrupt or degrade the backbone of the US and NATO information technology-enabled warfare, critical infrastructures (C4ISR), including space-based systems, command and operational networks, and other complex technological warfare enablers that developed countries depend on. The Russian Aerospace Forces, created in 2015, integrate the previously separated offensive and defensive capabilities, including air defence, missile defence, offensive electronic warfare, anti-space capabilities (such as anti-satellite missiles and manoeuvring space robots),[123](https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090) and directed energy weapons, such as the abovementioned Peresvet.[124](https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090) They are likely to play key role in crisis and conflict, including regional war scenarios.

### Hypersonics Internal

#### Hypersonic development occurring right now and both China and Russia leads the race. AI implementation drastically improves targeting and potentially opens up pre-emptive nuclear strikes against other states.

EA Times 21 (The EurAsian Times Desk (ET Desk) comprises authors, reporters, interns, newswires, etc who directly work under the Editorial Desk of The EurAsian Times and senior Editors of the media house.) “Powered By ‘On The Fly’ Algo, China Says Its AI-Controlled Hypersonic Missiles Can Hit Targets With 10 Times More Accuracy” October 18, 202 1https://eurasiantimes.com/china-says-its-ai-hypersonic-missiles-can-hit-targets-with-10-time-more-accuracy/ // ZX

When it comes to hypersonic weapons, the US’ near-peer rivals Russia and China seem to be ahead in the race. This fact, coupled with the understanding that Beijing has been betting big on Artificial Intelligence (AI) for the modernization of its military leads to a whole new possibility — the potential use of AI for providing accuracy to hypersonic weapons. [The FT had reported](https://www.ft.com/content/ba0a3cde-719b-4040-93cb-a486e1f843fb) that “China tested a nuclear-capable hypersonic missile in August that circled the globe before speeding towards its target, demonstrating an advanced space capability that caught US intelligence by surprise.” The report quoted unnamed sources “briefed on the intelligence.” However, China’s Ministry of Foreign Affairs spokesperson Zhao Lijian said the August test was “a spacecraft, not a missile.” Earlier this year, US Strategic Command chief Charles Richard, speaking at the annual symposium on space defense, [acknowledged](https://eurasiantimes.com/zircon-missile-us-finally-admits-that-russia-is-the-world-leader-in-hypersonic-missile-technology/) that Russian hypersonic technology will provide the Russian Navy with an undeniable advantage. “Our current ground-based and space-based sensor system may not be able to cope with the detection and tracking of these missiles. I must admit that Russia is the world’s leading country in hypersonic technology. And if the enterprises of our defense industry in a short time do not figure out how to resist them, the ships of the fleets of the NATO countries will become vulnerable,” Richard said. China has been aggressively developing hypersonic weapons. It currently has two lethal hypersonic missiles – the Dong Feng-17 (DF-17) and the DF-ZF Hyper Glide Vehicle (HGV). The former is a medium-range missile or MRBM system equipped with an HGV. It can carry conventional as well as nuclear weapons and has a reported range of 1,800-2,500km and a launch weight of 15,000kgs. The second is the DF-ZF HGV that can travel at speeds between Mach 5 and 10. It is apparently capable of performing “extreme maneuvers” to evade enemy defenses. The DF-17 has been designed to work specifically with the DF-ZF, exponentially amplifying both these weapons’ powers. In addition to developing these advanced weapons, researchers from the PLA have reportedly made some changes to the software, enabling them to land [hypersonic drones.](https://eurasiantimes.com/hypersonic-race-with-us-and-russia-china-learns-to-land-its-ultra-fast-missiles/) Now, its researchers are looking at the integration of AI with these ultra-fast munitions. China’s military leadership has recognized that AI (artificial intelligence) and similar technologies including machine learning, neural networking, human-machine teaming, and autonomous systems (also referred to as ‘intelligentised weapons’) are crucial for achieving a headstart in next-generation warfare. President Xi Jinping has mandated a “full modernization” of China’s People’s Liberation Army (PLA) by 2035. His government aims to put the Chinese military on par with the US military by 2050. To that end, the PLA is making headway into the [research, development, and operationalization of AI](https://www.orfonline.org/expert-speak/how-china-aims-to-augment-its-military-strength-using-ai/) for military utilization. Several laws and initiatives have been put in place to aid this endeavor. For instance, the National Security Law (2015) and National Intelligence Law (2017) compel all Chinese organizations and citizens to help facilitate the establishment’s efforts. Meanwhile, the Civil-Military Fusion (CMF) aims to make use of the resources and research capabilities of the country’s privately-owned companies, universities, and research institutions to the defense forces’ advantage. [SCMP reported](https://www.scmp.com/news/china/military/article/3152179/china-military-researchers-pinpoint-ai-hypersonic-weapons#:~:text=Their%20study%20showed%20an%20AI,10%20metres%20(32%20feet).&text=Based%20on%20this%20fresh%20information,cruising%20stage%20of%20hypersonic%20flight.) that PLA missile scientists had said the accuracy of hypersonic weapons could be improved by more than 10 times if control is given to a machine. Xian Yong and Li Bangjie, professors at College of War Support, Rocket Force Engineering University, said more decision-making power would be handed to the smart weapon. This would leave its human controllers with no clue as to how the weapon would behave after it had been launched. However, they claimed that overall positioning accuracy “would increase by one to two orders of magnitude”. Their paper proposes using AI to write the weapon’s software “on the fly”, while it moves at hypervelocity, through a unique flight control algorithm. Using their method, the AI would start calculating immediately after launch, even before the weapon reaches hypervelocity, to compute its position using the signal from the GPS. These results would then be compared with the results generated by the onboard sensors to evaluate the actual condition of the hardware. Relying on this new information, the AI would create a unique positioning algorithm for the weapon’s flight control program even before it entered the cruising stage of hypersonic flight.

#### Hypersonics destabilize defensive capabilities and cannot be blocked by missile defense. Future development could lower costs and see use in conjunction with nuclear warheads.

Boyd 4/15 (Iain D. Boyd is the H.T. Sears Memorial Professor in the Department of Aerospace Engineering Sciences, and Director of the Center for National Security Initiatives at the University of Colorado. He received a Ph. D. in aeronautics and astronautics (1988) from the University of Southampton in England. He worked for four years at NASA Ames Research Center in the areas of aerothermodynamics and space propulsion.) “How hypersonic missiles work and the unique threats they pose – an aerospace engineer explains” April 15, 2022 [https://theconversation.com/how-hypersonic-missiles-work-and-the-unique-threats-they-pose-an-aerospace-engineer-explains-180836 //](https://theconversation.com/how-hypersonic-missiles-work-and-the-unique-threats-they-pose-an-aerospace-engineer-explains-180836%20//) ZX

Russia [used a hypersonic missile](https://www.cnn.com/europe/live-news/ukraine-russia-putin-news-03-19-22/h_e258f4d62704c278417a897db16cac80) against a Ukrainian arms depot in the western part of the country on March 18, 2022. That might sound scary, but the technology the Russians used is not particularly advanced. However, next-generation hypersonic missiles that Russia, China and the U.S. are developing do pose a significant threat to national and global security. I am an [aerospace engineer](https://scholar.google.co.uk/citations?user=0vO6w7MAAAAJ&hl=en) who studies space and defense systems, including hypersonic systems. These new systems pose an important challenge due to their maneuverability all along their trajectory. Because their flight paths can change as they travel, these missiles must be tracked throughout their flight. A second important challenge stems from the fact that they operate in a different region of the atmosphere from other existing threats. The new hypersonic weapons fly much higher than slower subsonic missiles but much lower than intercontinental ballistic missiles. The U.S. and its allies do not have good tracking coverage for this in-between region, nor does Russia or China. Russia has claimed that some of its hypersonic weapons can carry a nuclear warhead. This statement alone is a cause for concern whether or not it is true. If Russia ever operates this system against an enemy, that country would have to decide the probability of the weapon being conventional or nuclear. In the case of the U.S., if the determination were made that the weapon was nuclear, then there is a very high likelihood that the U.S. would consider this a first strike attack and respond by [unloading its nuclear weapons on Russia](https://www.britannica.com/topic/second-strike-capability). The hypersonic speed of these weapons increases the precariousness of the situation because the time for any last-minute diplomatic resolution would be severely reduced. It is the destabilizing influence that modern hypersonic missiles represent that is perhaps the greatest risk they pose. I believe the U.S. and its allies should rapidly field their own hypersonic weapons to bring other nations such as Russia and China to the negotiating table to develop a diplomatic approach to managing these weapons. The primary reason nations are developing these next-generation hypersonic weapons is how difficult they are to defend against due to their speed, maneuverability and flight path. The U.S. is starting to develop a layered approach to defending against hypersonic weapons that includes a constellation of sensors in space and [close cooperation with key allies](https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/). This approach is likely to be very expensive and take many years to implement. With all of this activity on hypersonic weapons and defending against them, it is important to assess the threat they pose to national security. Hypersonic missiles with conventional, non-nuclear warheads are primarily useful against high-value targets, such as an aircraft carrier. Being able to take out such a target could have a significant impact on the outcome of a major conflict. However, hypersonic missiles are expensive and therefore not likely to be produced in large quantities. As seen in the recent use by Russia, hypersonic weapons are not necessarily a silver bullet that ends a conflict.

### Impacts – AI Good

#### AI will transform warfare – failure to effectively, and quickly, adopt AI platforms crushes NATO military readiness – cooperation now is key.

Christou ‘21 (George, 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. 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. 01/03/2021 https://www.iai.it/sites/default/files/978195445000.pdf)

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.

#### AI key for future NATO deployment and training-visualization, analyzation, integration, equipment protection

Husain et al. 18(Amir Husain, August Cole, and Wendy R Anderson. CEO of Spark Cognition & Board of Adivisors for UT Austin’s Department of Computer Science & Member of Council on Foreign Affairs, Senior fellow of Scowcroft Center on Strategy and Security at the Atlantic Council & Fellow of Brute Krulak Center for Innovation and Creativity at Marine Corps University. " As Budget Polemic Drives Headlines, Do Not Lose Track of NATO’s Approach to AI". 07-27-2018. Royal United Services Institute. https://www.europarl.europa.eu/cmsdata/155282/WendyRAnderson\_RUSIArticle.pdf. 6-22-2022.)-cg

Indications and Warnings of Crisis Readiness at an Alliance level depends on the synchronized sharing of high-quality data to inform intelligence assessments and general situational awareness. One way to accomplish this is to establish AI-focused all-source data processing that is centralized by NATO headquarters but produced by, and available to, member states. An electronically shared view of the operational environment, frequently referred to as a common operating picture, can be developed in seconds, not days, to aid overloaded human analysts. Data sources must be expanded beyond conventional defense-related sources, to include open-source and commercially available imagery, metadata, and social media. Existing machine-learning systems already make this possible, but their use is nascent. The current generation of analytical software tools are a step in the right direction, but plenty of unprocessed data is not transformed into national and Alliance-level actionable intelligence reports due to a shortage of human analysts. This causes gaps in the intelligence picture, which can be exploited by an adversary. Taking full advantage of AI can smooth out the escalation of a crisis by combining the analytic efforts of NATO command organizations and member states to ascertain how, and when, a scenario will develop. Machine-learning crisis simulation systems offer improved visibility into the causes and drivers of a crisis that might otherwise be overlooked by conventional analysis, which can be too narrow to capture the true complexity of a situation. Integrating AI into coalition operations is a global challenge, not only for NATO, but also its supporting allies, many who, in the hyper war era, may not be organized militaries. In a hybrid, multi-domain context, a real-time common operating picture – that draws upon simulations but is also predictive – must extend into the information domain, including modelling peacetime public narratives. The volume and velocity of information during the early phases of a crisis will be nearly overwhelming. Anything other than an AI system has little hope of success in keeping up, while paring away irrelevant information to ensure that human decision-makers are tracking the right information. As with the assessment phase, AI-driven simulations and scenario planning offer substantial insights. With those insights, such systems can create a comprehensive picture of force readiness and logistical imperatives to inform NATO’s response options. AI-driven analysis can process massive amounts of unstructured data, maintenance logs, reports, and logistical information to create a detailed and accurate picture of force readiness. Machine-learning systems can also fold-in data from civilian, commercial-sector and non-governmental sources in order to produce a more accurate ‘whole of society’ capabilities view than what is currently possible. Employing this approach across the 29 NATO states is especially critical in the context of high-intensity conflict scenarios that, although unlikely, would be potentially catastrophic. Additionally, being able to include civilian resources and infrastructure as part of this response option analysis is something that AI systems are better suited to do than conventional database analysis. In addition to readiness driving response options, another major consideration is developing plans and evaluating their effectiveness. In more tactical scenarios, such as in the development of mission optimized auto-pilot capabilities for fighter aircraft, AI techniques such as reinforcement learning are already proven in creating optimized operational plans for a single platform in a similar way that can be applied for entire combat elements. The operational execution of a plan by NATO forces is currently dependent on mere assumptions of the consistency of training, resources, and the joint force’s ability to accomplish their mission. AI, particularly when combined with virtual- and augmented-reality visualization, can play a significant role in providing advanced training and pre-deployment unit-level preparation for NATO-led forces during peacetime, to ensure a rapid yet smooth transition into conducting operations. During those operations, autonomous software can be used to assist with maintenance, logistics management, and targeting of offensive and defensive systems. It can also ensure that a NATO force is successfully integrated with autonomous, unmanned ground, air and sea vehicles to provide a standardized, and ever increasing, level of operational competence and consistency of execution. During operations, machine-learning systems can use sensor data, entire technical libraries, and advanced models to accurately predict and then prevent equipment failure; given the danger now posed by improvised explosive devices and precision munitions to supply lines, such efficiency has profound strategic importance. In more tactical scenarios, such as in the development of mission optimized auto-pilot capabilities for fighter aircraft, AI techniques such as reinforcement learning, which allows machines to share their experiences and optimal solutions among themselves, have shown their utility. Adversarial AI systems running within a simulator can assist in the evolution of a highly optimized, robust mission intelligence that is effective at fulfilling defined objectives. In a similar vein, adaptations of these tactical AI-driven simulator frameworks can be used to gauge likely public reactions to proposed response options. What all of these approaches permit is to potentially identify – and address – operational pitfalls before they actually occur. Given the importance of public opinion and political support for NATO, what happens after a crisis is as important as the operations undertaken during it. Disengagement is likely to be an ongoing real-time competition over information and digital narratives, as contested as an operation’s military elements. The AI tools will be familiar, not unlike the machine-learning algorithms that today automatically run behind the-scenes markets placing political ads or marketing campaigns onto social media feeds.

### Impacts – NATO

#### Russia will exploit divisions between NATO members to instigate nuclear crises---extinction.

Kulesa ’18 [Lukasz; February 2018; Research Director at the European Leadership Network; European Leadership Network, “Envisioning a Russia-NATO Conflict: Implications for Deterrence Stability,” <http://www.jstor.com/stable/resrep17437>]

Escalation: Can a NATO - Russia conflict be managed?

Once a conflict was under way, the “fog of war” and rising unpredictability would inevitably set in, complicating the implementation of any predetermined theories of escalation, deescalation and inter-conflict management. The actual dynamics of a conflict and the perceptions of the stakes involved are extremely difficult to predict. Simulations and table-top exercises can give only limited insights into the actual decision-making processes and interactions. Still, Russian military theorists and practitioners seem to assume that a conflict with NATO can be managed and controlled in a way that would bring it to a swift end consistent with Russian aims. The Russian theory of victory would seek to exploit weak points in an Alliance war effort. Based on the conviction that democracies are weak and their leaders and populations are risk-averse, Russia may assume that its threats of horizontal or vertical escalation could be particularly effective. It would also try to bring home the notion that it has much higher stakes in the conflict (regime survival) than a majority of the NATO members involved, and thus will be ready to push the boundaries of the conflict further. It would most likely try to test and exploit potential divisions within the Alliance, combining selective diplomacy and activation of its intelligence assets in some NATO states with a degree of selectivity in terms of targets of particular attacks. Any NATO-Russia conflict would inevitably have a nuclear dimension. The role of nuclear weapons as a tool for escalation control for Russia has been thoroughly debated by experts, but when and how Russia might use (and not merely showcase or activate) nuclear weapons in a conflict remains an open question. Beyond catch phrases such as “escalate to de-escalate” or “escalate to win” there are a wider range of options for Russian nuclear weapon use. For example, a single nuclear warning shot could be lethal or non-lethal. It could be directed against a purely military target or a military-civilian one. Detonation could be configured for an EMP effect. A “false flag” attack is also conceivable. These options might be used to signal escalation and could significantly complicate NATO’s responses. Neither NATO nor its member states have developed a similar theory of victory. Public NATO documents stipulate the general goals for the Alliance: defend against any armed attack and, as needed, restore the full sovereignty and territorial integrity of member states. It is less clear how far the Alliance would be willing to escalate the conflict to achieve these goals, and what mechanisms and means it would use while trying to maintain some degree of control over the conflict. The goals and methods of waging a conflict with Russia would probably have to be limited in order to avoid a massive nuclear exchange. Such limitations would also involve restrictions on striking back against targets on Russian territory. But too narrow an approach could put too much restraint on NATO’s operations: the Russian regime’s stability may ultimately need to be threatened in order to force the leadership into terminating the conflict. NATO would thus need to establish what a proportional self-defence response to Russian actions would involve, and to what extent cyber operations or attacks against military targets in quite different parts of Russia would be useful as tools of escalation to signal NATO’s resolve. Moreover, individual NATO Allies, especially those directly affected by Russia’s actions, might pursue their individual strategies of escalation. With regards to the nuclear dimension in NATO escalation plans, given the stakes involved, this element would most likely be handled by the three nuclear-weapon members of the Alliance, with the US taking the lead. The existence of three independent centres of nuclear decision-making could be exploited to complicate Russian planning and introduce uncertainty into the Russian strategic calculus, but some degree of “P3” dialogue and coordination would be beneficial. This coordination would not necessarily focus on nuclear targeting, but rather on designing coordinated operations to demonstrate resolve in order to keep the conflict below the nuclear threshold, or bring it back under the threshold after first use. Relying on concepts of escalation control and on lessons from the Cold War confrontation might be misleading. The circumstances in which a Russia-NATO conflict would play out would be radically different from the 20th century screenplay. Moreover, instead of gradual (linear) escalation or salami tactics escalation, it is possible to imagine surprizing “leap frog” escalation, possibly connected with actions in different domains (e.g. a cyberattack against critical infrastructure). Flexibility, good intelligence and inventiveness in responding to such developments would be crucial. Conflict termination Russian and NATO assumptions regarding conflict termination would most likely not survive the first hours of an actual conflict. Both sides are capable of underestimating the resolve of the other side to prevail in a conflict and the other side’s willingness to commit the necessary resources and endure the costs, especially once both sides start committing their political capital and resources and the casualties accumulate.

### Impact – Russia

#### Unless stopped, Putin will escalate – extinction

Dokoupil 22 – Tony Dokoupil is an American broadcast journalist and author, known for his work as a co-anchor of CBS Mornings. He was also a news correspondent for CBS News and MSNBC. (Tony Dokoupil, "Conflict in Ukraine triggers fear of nuclear warfare," CBS, 4-29-2022, https://www.cbsnews.com/news/conflict-nuclear-warfare-ukraine-russia/, Accessed 6-21-2022, LASA-SC)

The threat of a global nuclear war doesn't feel as distant as it did a few weeks ago. A recent CBS News poll found that 70% of adults are worried Russia's invasion of Ukraine could lead to fighting with nuclear weapons. Many are curious as to what a nuclear war would look like — so Alex Wellerstein, a historian and professor at the Stevens Institute of Technology, developed a website called "NUKEMAP." It can simulate a detonation anywhere in the world. As in real life, the simulation begins with just the push of a button. CBS News' Tony Dokoupil and Wellerstein simulated a scenario of what Times Square would look like if it was hit with a bomb like the one that struck Hiroshima. "There's a sort of zone that's about here, and... which is pretty hopeless, no matter what," Wellerstein said as he pointed to a large section of midtown Manhattan in the simulation. When larger, more modern bombs were simulated, the website showed a single blast could cause heavy damage throughout the entire metropolitan region and kill millions. Winds can also carry radioactive particles even further. "These are areas where, if you're not taking shelter several hours after the bomb, you could get enough radiation to die," Welllerstein said when referring to cities downwind of New York in the simulation. "You could get enough radiation to get significantly sick." There was a time when Americans were prepared for that kind of attack. In the 1950s and 60s, school children practiced "duck and cover" drills to help survive a blast, and a public campaign educated Americans on surviving the fallout. Office of Civil Defense teams also spent hundreds of millions of dollars building and stockpiling fallout shelters all across the U.S., but a visit to the basement of a public library in Passaic, New Jersey, reveals this threat has fallen into the very back of our minds. In a space that was designed to shelter up to 90 people, decades of dust has settled over the medicine and food — which has long since expired — in the basement. Building supervisor Gary Salvatoriello told CBS News there are no plans for replenishment. Instead, the one-time fallout shelter, like so many others, has turned back into an everyday storage space. George Washington University professor Sharon Squassoni said she's been warning about the risk of nuclear conflict for years. "The lessons of the Cold War seem to have been forgotten," she said. The number of nuclear weapons has decreased dramatically since the Cold War. But Russia and the U.S. each have more than 1,500 weapons deployed and ready to fire. Squassoni said she fears that could happen eventually, either by accident or an intentional attack. "We know from Russian doctrine that they have a plan or they've been thinking about using nuclear weapons to escalate the war, to stop it or deescalate it," she said. The big question is: what would happen after an initial attack? "The world would recoil in horror. And I'm sure there would be a lot of voices demanding for some kind of similar action. But do you really want to trigger the third world war? A third nuclear war?" Squassoni said. "I don't think that Vladimir Putin wants to tangle with NATO," she added. "I don't think he wants to tangle with the U.S. But I also think that we've been misreading him for quite a while. The truth is there is very little standing in the way of an all-out nuclear war. "The only thing that really stands is that... it is not really in the interests of our enemies to have that happen to them either," Wellerstein said. Even though nuclear weapons haven't been used in battle since 1945, Wellerstein said the threat they post never really went away. "We have a long list of stuff to worry about. But I think they should be on the list. I'm not saying they should be the top of the list all the time. But I think if they were on the list, you might get a somewhat different world as a result," he said. "Future problems are brewing, I guarantee it."

#### Nato is key to deterring Putin--- collapse causes global insecurity.

Ilya Timtchenko 03-21-2022 [Ilya Timtchenko is studying public policy at the Harvard Kennedy School and is chair of the Ukraine Caucus, a student organization at the Harvard Kennedy School. He was previously an editor at the Kyiv Post, Atlantic Council, “Fear of provoking Putin is leading the Western world toward disaster,” https://www.atlanticcouncil.org/blogs/ukrainealert/fear-of-provoking-putin-is-leading-the-western-world-toward-disaster///ZW]

The conventional wisdom in Washington is that NATO should refrain from enforcing a No-Fly Zone over Ukraine due to the risk of an all-out NATO-Russia war. This view reflects a decades-long misunderstanding of both Russia and Ukraine, and is mired in appeasement thinking. While the window to impose a No-Fly Zone has likely closed, there are still alternatives that could work. The West should implement them without delay. After the 1991 collapse of the Soviet Union, the US hastily abandoned the post-Soviet world and moved on to other international challenges. Ironically, this disinvestment meant that it stopped maintaining and developing the very expertise that had allowed America to triumph over the USSR in the first place. Over the intervening three decades, appeasement has replaced expertise. Whether it was Russia’s brutal wars in Chechnya, the 2008 war with Georgia, or the 2014 invasion of Crimea and eastern Ukraine, the West’s approach has frequently been shaped by fear of provoking an already aggrieved Russia. This has led the West to misread Putin’s Russia again and again. It also caused Western leaders to misinterpret developments in Ukraine. We overestimate Putin and underestimate Ukraine due to limited understanding of the fast-changing dynamics in the post-Soviet region. The West’s dangerous disregard for the threat posed by a revanchist Kremlin explains why the democratic world did not maintain its advantage over Russia when the latter was most vulnerable. The fall of the Soviet Union provided a golden opportunity for rapid NATO expansion, including into Ukraine. While it is fashionable to claim NATO enlargement went too far, in the current circumstances it makes far more sense to argue that it did not go far enough. Thankfully, it is not too late for the West to learn from its mistakes. While Russia has significantly greater military power today than in the 1990s, it is still no match for NATO, and Putin will not fight if challenged by the collective might of the West. NATO could coordinate with non-NATO nations to protect Ukraine’s skies, especially as the Biden Administration has demonstrated its ability in recent weeks to unify the world against Russia. America could theoretically mobilize a broad coalition to protect Ukraine. In the current extreme circumstances, there is no reason why the global community cannot adopt a creative approach to save a country that has been blatantly attacked by a permanent member of the UN Security Council and has stunned the world with its heroism. Retired four-star General in the United States Air Force Phil Breedlove has stated that a No-Fly Zone must be on the table. He also suggested an alternative: a humanitarian No-Fly Zone. This is a potentially attractive idea that could serve as a compromise between advocates of a cautious policy towards the Kremlin and those who believe Russia will not ultimately escalate into open war with NATO. While Western leaders have so far been unambiguous in ruling out direct intervention, they are also providing Ukraine with enhanced anti-aircraft capabilities. Such measures need to be significantly speeded up and bolstered by the parallel provision of fighter jets and anti-missile defense systems. In less than four weeks of war, Russia has fired more than a thousand missiles at Ukraine and reduced entire Ukrainian cities to rubble. While the civilian death toll remains unconfirmed, many thousands are already feared dead. Despite the obvious urgency of the situation, the West is still acting in half-measures and contemplating if arming Ukraine could be interpreted as provocative by Putin. If Western leaders maintain their current cautious approach towards Russian aggression, the watching world will witness an unfolding genocide of the Ukrainian people. This will be joined by a rapidly escalating global food crisis. Russian tanks will not stop at Ukraine’s western borders. On the contrary, Putin will be emboldened to expand his wars of imperial aggression and will inevitably turn his attention to Moldova and the Baltic States while also seeking to destabilize Central Europe and the Balkans. Meanwhile, China and other authoritarian powers will take note of Putin’s success and act accordingly. They will forge closer ties with a resurgent Russia and will seek to expand their own spheres of influence in a similar manner. The entire world will enter into a new era of global insecurity that will reverse much of the progress made since World War II. Rather than remaining reactive and paying an even greater price in the near future, NATO should act decisively now and dramatically increase its support for Ukraine. To do otherwise is not only immoral; it is against the core strategic interests of the entire Western world.

#### Russia war causes extinction

Owen Cotton-Barratt et al. 17 - PhD in Pure Mathematics, Oxford, Lecturer in Mathematics at Oxford, Research Associate at the Future of Humanity Institute; “Existential Risk: Diplomacy and Governance,” <https://www.fhi.ox.ac.uk/wp-content/uploads/Existential-Risks-2017-01-23.pdf>

The bombings of Hiroshima and Nagasaki demonstrated the unprecedented destructive power of nuclear weapons. However, even in an all-out nuclear war between the United States and Russia, despite horrific casualties, neither country’s population is likely to be completely destroyed by the direct effects of the blast, fire, and radiation.8 The aftermath could be much worse: the burning of flammable materials could send massive amounts of smoke into the atmosphere, which would absorb sunlight and cause sustained global cooling, severe ozone loss, and agricultural disruption – a nuclear winter. According to one model 9 , an all-out exchange of 4,000 weapons10 could lead to a drop in global temperatures of around 8°C, making it impossible to grow food for 4 to 5 years. This could leave some survivors in parts of Australia and New Zealand, but they would be in a very precarious situation and the threat of extinction from other sources would be great. An exchange on this scale is only possible between the US and Russia who have more than 90% of the world’s nuclear weapons, with stockpiles of around 4,500 warheads each, although many are not operationally deployed.11 Some models suggest that even a small regional nuclear war involving 100 nuclear weapons would produce a nuclear winter serious enough to put two billion people at risk of starvation,12 though this estimate might be pessimistic.13 Wars on this scale are unlikely to lead to outright human extinction, but this does suggest that conflicts which are around an order of magnitude larger may be likely to threaten civilisation. It should be emphasised that there is very large uncertainty about the effects of a large nuclear war on global climate. This remains an area where increased academic research work, including more detailed climate modelling and a better understanding of how survivors might be able to cope and adapt, would have high returns. It is very difficult to precisely estimate the probability of existential risk from nuclear war over the next century, and existing attempts leave very large confidence intervals. According to many experts, the most likely nuclear war at present is between India and Pakistan.14 However, given the relatively modest size of their arsenals, the risk of human extinction is plausibly greater from a conflict between the United States and Russia. Tensions between these countries have increased in recent years and it seems unreasonable to rule out the possibility of them rising further in the future.

### AT: Deterrence Turn

#### AI systems are inevitable – if China and Russia develop them, it still undercuts balance of power and triggers this turn, better for US deterrence to remain credible.

#### AI systems are vital to overall deterrence postures and replacing conventional systems with reliable second-strike and self-isolating military capabilities.

Horowitz 19 (Michael C. Hororwitz is a former Adjunct Senior Fellow in the Technology and National Security Program at CNAS. Michael C. Horowitz is Richard Perry Professor and the Director of Perry World House at the University of Pennsylvania. He is also an adjunct senior fellow at the Center for a New American Security. His research interests include technology and global politics, military innovation, the role of leaders in international politics, and forecasting.) May 2019 “Artificial intelligence and nuclear stability” THE IMPACT OF ARTIFICIAL INTELLIGENCE ON STRATEGIC STABILITY AND NUCLEAR RISK Volume I Euro-Atlantic Perspectives p.60-70 <https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf>) // ZX

Nuclear-armed states, and also non-nuclear-armed states, could use machine learning and autonomy in non-nuclear applications with a strategic effect. Machine learning methods could significantly improve the targeting capability of conventional defensive systems. Missile and air defence systems have relied on automation for decades. The first automatic air defence system, the Mark 56 gun fire-control system, was invented during World War II.24 Since the 1970s, air defence systems have been using an AI technology known as automatic target recognition (ATR) that can detect, track, prioritize and select incoming air threats more rapidly and more accurately than a human possibly could. However, the progress of the target-identification capabilities of these systems has been slow, particularly due to the difficulties associated with the development of target libraries (i.e. the database of target signatures that an ATR system uses to recognize its target). With traditional AI programming methods, the designers of an ATR system have to upload a large and representative sample of data about the target in all conceivable variations of its operating environment (i.e. background and weather conditions). This is a challenging task for many target types and operational situations.25 Advances in machine learning, particularly deep learning and generative adversarial networks (GANs), could significantly simplify that process.26 With deep-learning methods, engineers could make ATR systems capable of learning independently not only the differences between types of target but also the differences between military and civilian objects (e.g. a commercial aeroplane and a strategic bomber).27 With GANs, engineers could generate realistic synthetic data on which an ATR system can be trained and tested in simulation. An ATR system trained with these machine learning techniques would perform comparatively much better than an ATR system trained with traditional methods. Equally, autonomous systems offer new defensive tools against incoming threats. Autonomous unmanned vehicles can be deployed as decoys or flying mines to complement traditional air defences.28 Advances in autonomy for swarming and for multi-vehicle control could also enable autonomous unmanned systems to operate in a coordinate way and conduct advanced A2/AD manoeuvres.29 Such systems would increase deterrence against both conventional and nuclear attack as they would increase the risks for an attack by manned platforms (e.g. combat aircraft and manned bombers) and make the outcome of an attack with unmanned systems (including missiles) more uncertain.

## Cooperation Advantage

### NATO Solves

#### 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.

#### 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 multilateral coop solves – allows for innovation and responsible use**

**Mahoney 4-30** [Casey Mahoney, Casey Mahoney is a U.S. Institute of Peace–DoD Minerva Peace & Security Scholar and a Ph.D. Candidate in political science at the University of Pennsylvania. He served as a Nunn-Lugar Fellow in the Office of the Secretary of Defense for Policy and in AT&L from 2013 to 2017. , 4-30-2022, accessed on 6-26-2022, The National Interest, "Shared Responsibility: Enacting Military AI Ethics in U.S. Coalitions", https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/shared-responsibility-enacting?page=0%2C1]//PJ

In March 2021, Google’s Eric Schmidt and former Department of Defense (DoD) deputy secretary Bob Work wrote in their preface to the 756-page report of the bipartisan National Security Commission on Artificial Intelligence (NSCAI), “America is not prepared to defend or compete in the AI era.” As chair and vice-chair of the NSCAI, respectively, they summarized the commission’s solution: “America needs to enlist its oldest allies and new partners to build a safer and freer world for the AI era.” Though the U.S. military is taking pains to ensure AI does not erode its ideal to fight wars ethically, it cannot afford to leave its allies and partners behind in this endeavor. DoD is working to ensure the U.S. military can deter and fight AI-infused armed conflicts as part and likely leader of future coalitions using ethical, or “responsible,” AI. Efforts have focused on establishing broad principles for AI development and use and have targeted the technical enablers of multinational uses of AI, like standardizing data-labeling processes and pursuing data-sharing agreements with partners. This is not enough. On the coalition battlefield, the ethics of military AI come down to the choices leaders and commanders make about how to use AI-enabled weapons. But it is not clear that coordination and joint decisionmaking practices at the political and operational levels used in U.S.-led coalitions to date are well-suited to operations in an AI era. How will coalitions manage a more complex decision space, where different nations’ AI systems pass algorithm outputs to operators and analysts across a coalition? Will decisionmaking outcomes be consistent with our ethical ideals? AI is making human judgment in war more, not less, important. This means the United States and its allies and partners will need to innovate together, focusing on more than broad ethical principles and technical solutions. The U.S. defense enterprise can take three concrete steps I describe below to ensure its own and its partners’ technology and ideals align with the organizational structures—that is, in coalitions—in which AI-enabled weapons will be put to use. Foundations of AI Responsibility in U.S. Alliances and Partnerships Because the United States fights in coalitions in most armed conflicts, focusing on developing partnerships to integrate military AI is a prudent approach. The NSCAI charged the DoD with achieving broad military AI readiness by 2025, including by “promoting AI interoperability with allies and partners,” and the Pentagon is heeding this call. In September 2020, DoD had already convened representatives from thirteen countries from NATO, non-NATO alliances, and other defense partnerships to socialize its ethical principles for AI and coordinate on military AI ethics policy. This AI Partnership for Defense (AIPfD) aims to “promote the responsible use of AI, advance shared interests and best practices … establish frameworks to facilitate cooperation, and coordinate strategic messaging.” Since then, engagement with international defense partners has broadened and deepened. By June 2021, AIPfD had added three additional member states to the group; in March 2022, it convened its fifth international dialogue. AIPfD cooperation has deepened from high-level conversations to discussions on AI-use scenarios, marking progress toward a key NSCAI recommendation the DoD focus on specific AI use-cases in exercises and wargames. In addition, in October 2021, NATO adopted an alliance-wide AI strategy focused mostly on responsible use. Biden administration initiatives in the Indo-Pacific in 2021—reinvigorating the Quadrilateral Security Dialogue (Quad) with Australia, India, and Japan and concluding the Australia-U.K.-U.S. (AUKUS) technology-sharing agreement—also targeted AI cooperation. Early work in the Quad has included collaboration on AI technical standards more generally, while AUKUS members are cooperating on capabilities for use in contested military environments. Finally, U.S. military services have also begun incorporating new AI systems into multinational operational exercises, experimentation that can help foresee and overcome the technical and operational challenges of using novel technology in coalitions. Important early steps like these help enact standards, like keeping humans in AI systems’ decision loops and having strong technology-policy review processes, meant to avoid worst-case scenarios where uncontrolled, unvalidated systems are fielded in armed conflict. But, the Department has more to do to avoid the misuse or failure of AI-enabled weapons in future coalition operations. Whether the employment of any weapons system in armed conflict is “ethical” or “responsible” ultimately depends on the assessments commanders and political leaders make. In multinational operations with AI tools at the “tip of the spear,” non-U.S. leaders and commanders will also be faced with choices that determine whether they use such tools to enact values, like proportionality and discrimination, in fighting alongside U.S. forces. It is in the U.S. interest that they do this. Guaranteeing that they do, however, is difficult. Strength In Diversity? Many of the national AI strategy documents of NATO allies and U.S. allies and partners in the Indo-Pacific prioritize responsible governance over AI in and, in some cases, AI-enabled warfighting. This apparent, high-level harmony notwithstanding, public polling data from 2019 and 2021 suggest that among U.S. security partners, specific concerns about the use of lethal autonomous weapons systems vary widely. Data from this year show that the public’s trust in AI more generally varies from quite high among some partners, as in India and Turkey, to quite low, among traditional NATO allies and Japan. U.S. leaders should thus not assume their allies will be reading from an identical political or ethical playbook in future coalition operations with AI in the mix. Once shooting begins, coalition members frequently find they actually disagree about the policies and strategies that should guide operations. Domestic politics are often what shape the scope and limits of coalition members’ contributions to operations, and they can impact leaders’ strategic decisions in complex ways. This makes it worth thinking carefully about the benefits and risks of working in a coalition where views about military AI use and governance vary. Intuitively, a diversity of perspectives is useful for creative problem-solving. In plotting a course for research and development on military AI, DoD set the goal of building “a robust national and global [responsible AI] ecosystem” among partner government, private sector, and academic institutional partners to maximize creative potential and interoperability. In operational contexts, however, the stakes of navigating differences of the ethical frameworks and policies that inform leaders’ and commanders’ decisions are much higher. Without appropriate ways of managing coalition contributions, unforeseen mismatches in the skill levels and specialized capabilities of partner forces can have major negative effects on military effectiveness. National political differences about whether AI collaboration should be civilian- or military-focused, varied timelines over which militaries are adopting AI, and incompatibilities in legal and regulatory structures could all present challenges to U.S.-led coalitions cohesively enacting shared notions of military AI ethics. Is there a way to find operational strength in this diversity? A Responsible AI Coalition It is in the U.S. interest to leverage the creative potential of a diverse AI “ecosystem.” However, it is also necessary to establish habits that mitigate the risk that political, cultural, and organizational differences among future coalition partners might undermine collective, responsible AI use. To do this, the Defense Department can take steps now to increase the reliability with which future coalitions will operationalize the foundations of international cooperation on military AI. The DoD should pursue the three objectives and consider specific actions to pursue them. Building these goals into the charter of the DoD’s new Office of the Chief Data and AI Officer (CDAO) that Deputy Secretary Kathleen Hicks directed be prepared by June 1, 2022, would help align institutional incentives to accomplish them. Despite China’s efforts to lead in setting international AI technical standards, it is clearly in the U.S. interest to pursue its own standards under which it collaborates with military partners. The DoD should task the CDAO to oversee a process to identify what resources would be necessary to engage partners to develop and baseline U.S. programs around a technical glossary for AI. Doing so would set the terms of debate among the international partners DoD seeks to recruit to the responsible AI ecosystem it seeks to establish. Without shared language, communicating about partners’ capabilities and intent to use AI responsibly will be difficult, posing risks for the strategic effectiveness and political cohesion of future coalitions. Until now, the department has not needed to understand how its vast network of partner governments and militaries are absorbing a general-purpose technology like AI. A February 1 DoD memorandum identifies roles the CDAO and the undersecretaries for Policy, Acquisition and Sustainment (A&S), and Research and Engineering (R&E) will play in international cooperation on AI. But, DoD lacks a cross-cutting process for collecting technical and policy knowledge derived from these international interactions and integrating it into coalition policy, planning, or technical cooperation efforts on a country-by-country or weapons system-by-system basis. The DoD should task the CDAO, Policy, A&S, and R&E offices to create one. These offices should establish metrics in R&D, TEVV, and acquisitions processes that incentivize the bureaucracy to prioritize technical and organizational interoperability and consider unique requirements that might arise from ethical or policy questions likely to arise in multinational use scenarios. This would help channel international partner input to relevant points of contact across the department, optimizing the value of the international “responsible AI ecosystem” to U.S. coalition efforts. As China and Russia continue to use AI tools to enhance authoritarian control at home, it is becoming commonplace to argue that the values America and its allies share for responsible AI can represent a competitive edge of soft power. This might well be the case. Only if America and its allies are capable of enacting these values on the AI-infused battlefield together, though, will this advantage serve to help legitimize U.S.-led operations in the world’s eyes. A coalition’s ability to uphold the laws of armed conflict is ultimately bounded by the capability and willingness of its least able members to do so.

### China Authoritarianism

#### **China’s authoritarian ascendence will cause its downfall – the US will outcompete**

Kroenig 20 (Matthew Kroenig is a professor of government and foreign service at Georgetown University, and the deputy director of the Scowcroft Center for Strategy and Security at the Atlantic Council, “Why the U.S. Will Outcompete China,” The Atlantic, 4/3/2020, <https://www.theatlantic.com/ideas/archive/2020/04/why-china-ill-equipped-great-power-rivalry/609364/)-> MP

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. 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](https://www.amazon.com/Present-Creation-Years-State-Department/dp/0393304124) 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. 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](https://www.nytimes.com/2020/01/16/opinion/sunday/china-economy-trade.html) 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](https://www.newsweek.com/worlds-largest-economy-2030-will-be-china-followed-india-us-pushed-third-1286525) that China could even surpass the United States within the decade, and [some have suggested](http://content.time.com/time/world/article/0,8599,2043235,00.html) 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](https://www.fmprc.gov.cn/mfa_eng/ziliao_665539/3602_665543/3604_665547/t18011.shtml) only to nearly [fight a nuclear war](https://nsarchive2.gwu.edu/NSAEBB/NSAEBB49/index2.html) 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”](https://www.ft.com/content/05cd86a6-b552-11e7-a398-73d59db9e399) 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](https://aspi.gistapp.com/winter-2020/page/overview), 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](https://www.nytimes.com/2018/02/08/world/asia/south-china-seas-photos.html) from neighbors in the South China Sea and [conducting military exercises](https://www.nytimes.com/2017/07/25/world/europe/china-russia-baltic-navy-exercises.html) 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](https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf) 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](https://camphorpress.com/5000-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](https://www.bbc.com/news/world-asia-china-49317695) and Xinjiang—the CCP [spends more on domestic security](https://www.wsj.com/articles/china-spends-more-on-domestic-security-as-xis-powers-grow-1520358522) 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](https://www.theatlantic.com/ideas/archive/2020/03/china-trolling-world-and-avoiding-blame/608332/) 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](https://www.nytimes.com/reuters/2020/04/02/world/europe/02reuters-nato-northmacedonia.html). 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](https://www.nytimes.com/2020/03/19/world/asia/coronavirus-china-united-states.html) 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](https://time.com/5813628/china-coronavirus-statistics-wuhan/) the numbers of COVID-19 infections and [deaths](https://www.bloomberg.com/news/articles/2020-03-27/stacks-of-urns-in-wuhan-prompt-new-questions-of-virus-s-toll) in China, and European nations have [rejected](https://www.bbc.com/news/world-europe-52092395) and returned faulty Chinese coronavirus testing kits. The great political theorist Niccolò Machiavelli considered a similar line of thinking in the 16th century, about whether republics or dictators charted a more stable course. He wrote, “I, therefore, disagree with the common opinion that a populace in power is unstable [and] changeable … The prince … unchecked by laws, will be more … unstable, and imprudent than a populace.” The U.S. political system certainly has problems. But democracy is the best machine ever invented for generating enormous power, wealth, and prestige on the international stage.

### Misinformation

#### AI can be used to influence public ideology- control of online interaction

Kirdemir 19(Can Kasapoğlu, Bariş Kirdemir. Director of Security and Defense Studies at EDAM and Eisenhower fellow at NATO defense college."Artificial Intelligence and the Future of Conflict". 11-28-2019. Carnegie Europe. https://carnegieeurope.eu/2019/11/28/artificial-intelligence-and-future-of-conflict-pub-80421. 6-22-2022.)

New technologies encourage people, groups, and states to conduct influence operations and manipulation at scale. Intelligent machines can identify susceptible groups of people and “measure the response of individuals as well as crowds to influence efforts,” according to Rand Waltzman, deputy chief technology officer at RAND Corporation. Cognitive hacking, a form of attack that seeks to manipulate people’s perceptions and behavior, takes place on a diverse set of platforms, including social media and new forms of traditional news channels. The means are increasingly diversified, as distorted and false text, images, video, and audio are weaponized to achieve the desired effects. Cognitive security is a new multisectoral field in which actors engage in what Waltzman called “a continual arms race to influence—and protect from influence—large groups of people online.” AI could cause drastic changes in hybrid warfare, which is a major concern for NATO. States and nonstate actors can use cyberspace to influence large groups of civilians and opposing forces. From reconnaissance activities and the profiling of target audiences to the weaponization of distorted or fake information and psychological operations, AI broadens the potential of information operations. In addition, human-machine interactions will likely become a part of military engagements, with ethical and legal implications that remain unclear and unexplored. The introduction of this technology needs oversight to prevent potential abuses and unintended consequences. Another focus for NATO should be the values that the alliance has been defending for decades. As the use of AI in everyday life grows, biases and discrimination inherent in AI, the management of sensitive personal data, and malicious online behavior will change societies in ways that are only beginning to be understood.

### Ethical Framework

#### An AI ethical framework solves

Lockman and Trabucco 22 (​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. Lena Trabucco is a dual degree candidate pursuing a PhD in political science at Northwestern University and a PhD in Law at iCourts Center of Excellence in International Courts at the University of Copenhagen. “NATO’s Role in Responsible AI Governance in Military Affairs” March 2022, ,https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69)ZK

Introduction The introduction of artificial intelligence (AI) as a general-purpose technology has prompted analysts and researchers to reconsider the implications for warfare. As this Handbook edition illustrates, AI has, and will continue to, shape global dialogue, policy, and governance structures in international politics, including for future military operations. In this chapter, we explore a role for the North Atlantic Treaty Organization (NATO) in the emerging military AI governance architecture. NATO (or the Alliance) is a military and political alliance among 30 contributing member states that are committed to collective security. Much of NATO’s original purpose and current core tasks arguably leave the Alliance’s role uncertain in international governance regimes contending with the impact of emerging technology on international politics.1 As global powers compete for the economic and military capabilities that AI can offer, the Alliance has the enormously challenging task of navigating varying political realities and capabilities of Allies, all while effectively recalibrating strategic relationships in the coming years. Recognizing technological change as a key variable, NATO has begun to adapt its organizational composition and strategic footing to increase the Alliance’s capacity to meet emerging security challenges for military capability development trends of both its own members and those of competitors or adversaries. New power distributions around AI and adjacent dual-use technologies are among the motivating factors causing the Alliance to reconsider whether its technological superiority may be threatened in the years ahead, as reflected in the 2019 Emerging and Disruptive Technologies (EDTs) Roadmap2 and, more recently, the NATO 2030 process.3 NATO navigates these changes and then approaches AI-accelerated changes to the international security environment in a highly political context. Notably, in 2019, French President Emmanuel Macron surprised many European counterparts by declaring NATO “brain-dead,” a warning wrapped in an even larger warning of trans-Atlantic security divisions.4 The critique that NATO is a “brain-dead” or “irrelevant” institution has existed in some form since the end of the Cold War.5 As NATO combats global perceptions of organizational irrelevance, there is a reason to push for bureaucratic adaptation to better manage technology-driven changes in the future. As such, despite some warnings to the contrary, Allies have an incentive to keep NATO a relevant military institution and ensure that it adapts to emerging threats and for future military contexts. The comment from President Macron helped prompt the NATO 2030 agenda, which is currently taking shape to increase the Alliance’s role as a political actor and as an organization with a greater focus on EDTs.6 As NATO bodies and Allies prepare for the impact of AI on future military operations, the Alliance has its own responsibility to steward AI in ways that, inter alia, promote cohesion between democratic countries, prevent risks, shore up interoperability, project deterrence, and ensure stability.7 To achieve these aims, cooperation and alignment are critical for the Alliance to maintain a competitive edge and promote further innovation in alignment with shared values. With these incentives, we argue that an examination of NATO as a governance stakeholder is due to complement other literature on how humans, social structures, and institutions impact how technology develops. More specifically, this chapter borrows from two fields of scholarship that set the theoretical foundations for how institutions such as NATO impact technological trajectories, and thus have a responsibility to govern the technology accordingly. The two fields—science, technology, and society (STS) studies and military innovation literature—have different parameters, but both explore key questions that help establish the ways in which institutions exert their influence on the development, deployment, and diffusion of technologies like AI. We argue that this influence is a form of institutional power, building on Seth Lazar’s definition of governance in this handbook. Lazar writes that governance is “the use of power to make, implement, and enforce the constitutive norms of an institution.”8 In the context of this definition, this chapter examines AI governance as an instrument of power linking NATO’s responsibility and capacity to shape the future security environment in parallel to its own organizational interests. To be sure, NATO is far from the only institution that impacts military AI governance and its security implications. Indeed, international technology governance is inherently complex because it includes diverse stakeholders in a system of “organizations, regimes, and other forms of principles, norms, regulations, and decision-making procedures” with a shared interest and responsibility in a given issue-area of world politics.9 Existing discussions of the impact of AI on international security have looked to nation-states, regional institutions like the European Union (EU), or international bodies like the United Nations Convention on Certain Conventional Weapons (UN CCW) for discussions on the military governance of AI.10 Without expanding on the role of these other stakeholders, this chapter begins to explore pressing questions for NATO and international relations scholars that illustrate NATO’s role in AI governance, which has not had a comprehensive analysis.11 To begin to fill this gap, the analysis in this chapter centers on two AI governance mechanisms that NATO has at its disposal, and subsequently explores the Alliance’s capacity to use these mechanisms to exert its influence in key pillars of AI governance. Of the many possible AI governance mechanisms for NATO, this chapter offers a deeper assessment of two: (1) strategic and policy planning and (2) standards and certification. We fashion these mechanisms as primary components that connect NATO technology governance measures and responsible AI use.12 To illustrate NATO’s capacity to govern AI, we then examine three pillars, or foundational issue areas, which we believe represent critical elements of technology governance. We argue that, within each pillar, NATO is uniquely situated to facilitate cooperation via its governance mechanisms, with a view to shaping the future of AI for the Alliance and maintaining a competitive edge. Each pillar—(1) ethics and values, (2) legal norms, and (3) security and safety—is an area where researchers and analysts have acknowledged significant governance challenges, both at a national level and for international organizations like NATO. Each pillar, discussed in depth below, illustrates NATO’s potential as a governance stakeholder that can encourage multinational alignment on policy and standards for safer and better outcomes in future operations. The rest of this chapter continues as follows. First, we establish how STS studies and scholarship on military innovation focus on different aspects of technological advancement and governance outlooks. Second, this theoretical basis is applied to NATO to provide readers with an understanding of the institution’s entities and responsibilities related to AI governance. Next, the chapter discusses ways that NATO can leverage these mechanisms to ensure responsible use of AI in military operations based on ethics, law, safety, and security. Finally, the chapter concludes with reflections on NATO’s AI governance tools and, more broadly, roles for international organizations in the AI governance space. AI Governance and Military Affairs: Tensions in Existing Literature Academic literature has long grappled with the intersection of emerging technology and security organizations.13 Two branches of literature that tackle core questions of technological trajectories and its relationship to human and social structures—a critical question of governance for military technology—are STS studies and military innovation scholarship. Although the theoretical approaches in STS and military innovation studies differ, they both share the important assumption that technology does not have its own innate logic, and instead measure technological change by its impact on social structures and interactions with humans. In other words, both fields treat technology as an enabler in broader structures. The term technology is ubiquitous enough that it does not have a single definition, but it is often defined in relation to human intention and purpose. Alex Roland describes technology as a “purposeful human manipulation of the material world” to “serve some human purpose.”14 If extending this basic idea of technology to technological innovation, then both STS studies and military-innovation scholarship lend relevant criteria. Both academic fields are also relevant because, in the policy space, AI governance stakeholders are pursuing responsible research and innovation (RRI), which comes from STS studies, and defense stakeholders are similarly focused on responsible innovation and responsible use. More traditionally, the direct study of military adoption of technology is considered in the separate scholarship of military innovation, which includes a school of thought that focus on cultural and organizational factors. Between these two fields, an interdisciplinary approach is helpful here to carry STS approaches to AI governance, including RRI, over to the space of military innovation. However, this is complicated by the reality that military organizations that see technological superiority as a core element of deterrence and defense, including NATO, engage in forms of technological determinism that STS scholars squarely reject. Respective views on technological determinism—which considers that technology shapes society as a largely autonomous process with limited human agency—thus creates a tension for governance prospects.15 To spotlight the aspects of military innovation related to governance, this section briefly expands on the overlaps and tensions between STS and military innovation literature. Science, technology, and society (STS) studies STS studies is helpful to understand how technologies such as AI develop relative to the human, social, and political structures that shape it, rather than as an independent entity to which humans have to adapt.16 In this vein, AI is not just a computational process involving software, hardware, and data,17 so much it is a socio-technical system that encompasses “human, social, and organizational factors.”18 Together, these factors enable a focus on the trajectory of technological development relative to social structures and power dynamics. STS scholars have also helped develop RRI frameworks that seek to guide technological development in anticipatory, participatory, and adaptive frameworks to achieve desirable outcomes and prevent undesirable ones.19 RRI is a structured approach to innovation in which stakeholders identify and act on their “collective commitment of care for the future through responsive stewardship of science and innovation in the present.”20 It drives civilian AI ecosystems for NATO Allies that will also indirectly affect NATO.21 Responsible stewardship, or governance, of science and technology (S&T) requires stakeholders to change their approaches to technological development as the circumstances themselves change.22 In his book The Social Control of Technology, David Collingridge identified the double bind that makes technology governance (what he then referred to as social control) difficult: exerting social control or governing nascent technology is easy, but impossible because its evolution and eventual impacts are unknowable, and by the time the technology matures and its impact is realized, entrenched decisions will make future control more difficult.23 For now, AI remains a relatively immature technology, meaning circumstances will change as knowledge emerges and norms progressively develop. Collingridge also suggested the necessity of “corrigibility of innovation,” which refers to the “capacity to change shape or direction in response to stakeholder and public values and changing circumstances.”24 When applied to current RRI frameworks, the concept of corrigibility obligates governance stakeholders to shape the trajectory of a technology’s development and impact in ways based on social structures, both in anticipation of change and in response to decisions made in error.25 In short, stakeholders have to adopt corrigible practices to responsibly govern technology as it develops, and thus must claim their agency in guiding innovation even as technological development appears increasingly entrenched in previously made decisions and their subsequent outcomes. This is important for AI governance because technological advancement is making AI-accelerated risks clearer, including in the military space. Risks—especially as related to AI-enabled autonomous systems, poisoning of information environments, cyberattacks, unpredictable failure modes, and emergent behavior—will evolve in form and scale as the technology matures and diffuses. If AI evolution means more entrenchment and less corrigibility, the STS foundations remind governance stakeholders how to course-correct and adapt to changing risk assessments and the overall impact of AI in the international system.26 Nevertheless, while STS scholars study how decision-making that shapes the trajectory of technological innovation becomes entrenched, the field largely rejects the premise of technological determinism. Maintaining the centrality of human agency, as exerted also through social structures and institutions, is antithetical to determinist perspectives on technology developing on its own path independent of intervention. As Allan Dafoe, another contributor to this Handbook, has argued, the STS academic community’s refusal to engage with technological determinism severely limits STS applicability to empirics.27 As discussed below, this has implications for the ability of the STS field to impart responsibility to governance stakeholders in an area such as AI and international security. Military innovation literature The scholars that examine the way that military stakeholders manage technology and shape its development trajectory predominantly write on military innovation.28 These scholars measure technology adoption in changes to doctrine, organizational structures, and operational concepts, rather than seeing the technology as an end in and of itself.29 From this perspective, technology subsequently shapes human and social structures and organizations. To take an example similar to Roland’s definition of technology, Jonathan Shimshoni’s concept of “military entrepreneurship” involves the active manipulation of technology, doctrine, and war plans.30 In this sense, new technology adoption has tangible and observable effects on the operational environment. Similarly, Thomas Mahnken illustrates that military services shape technology to their respective purposes, rather than the other way around.31 The purpose that this manipulation, or molding, of technology serves is the creation, and ideally sustainment, of a comparative military advantage.32 Still, the way that this military advantage is defined is relevant here because metrics of success differ from other scholarship dealing with innovation. Military innovation importantly constitutes the relationship and social structures that form between technology and military bureaucracies. Yet as a field, it does not necessarily extend these relationships to their status as stakeholders in wider technology governance regimes.33 For instance, in his review of the different schools of military innovation, Adam Grissom offers a consensus definition of military innovation that inherently links it to effectiveness in the battlespace.34 Grissom clarifies that “measures that are administrative or bureaucratic in nature, such as acquisition reform, are not considered legitimate innovation unless a clear link can be drawn to operational praxis.”35 This reinforces the idea that technology on its own does not constitute an innovation if it is not observable in military operational practice or in battlefield advantage. The relatively narrow operational focus of military innovation scholarship means that management structures miss out on some of the uses of military power implicit in the governance of military technology. This means that both the bureaucratic entrenchment of technological advancement and the literature focusing on it do not necessarily address governance as an instrument of power in the military context. This may make sense for purely military technologies, but whether it discounts the agency that military bureaucracies have in governance of a pervasive, general-purpose technology like AI is worth separate consideration. As such, the operational measurement of the adoption and diffusion of technology as an instrument of military power likewise limits an understanding of how military technology management structures relate to governance. Implications for military AI governance Overall, STS offers much of the necessary groundwork for governance mechanisms and the impact of social structures on technology governance; however, it refuses to engage with technological determinism, or the independent influence of technology, that is often a driving force in military innovation. Recognizing that a comprehensive governance regime also needs to transpose to stakeholders that are engaged in the practices of governing AI, this study on NATO sees military innovation scholarship as a helpful complement to apply these STS foundations to practitioners’ perspectives. But scholarship on military innovation also has its own flaws, in that it looks at the management of technology exclusively formulated to exploit a comparative operational advantage. Measuring military innovation in relation to operational praxis makes sense to detect how military adoption of technology impacts operational excellence and upstream impacts on military strategy, but also makes it challenging for the empirics to apply to non-operational ways that military organizations exert their influence. Non-operational influence includes governance, the core topic that this chapter addresses. Despite differences, borrowing from the layered frameworks in STS and military innovation studies still helps contextualize innovation trajectories. Indeed, select scholars have attempted to bridge the gap between the social constructivist angle in STS studies and the technologically “optimistic”36 assumptions that frame technologically deterministic undercurrents, as seen in case studies on military innovation.37 Thomas Hughes examined these undercurrents in the defense sector as part of his theory of “technological momentum,”38 which argued military organizations are subject to inaction in S&T decision-making because the entrenchment of previous investments and decisions constrain the course of future technological development. Steven Fino expands on Hughes with the idea that “technological dislocations,” are an alternative reconciliation mechanism that acknowledges that technological determinism may operate beneath the surface of a technology’s maturation trajectory, while still allowing for socially driven perturbations that “dislocate” the “otherwise logical evolutionary patterns” of that technology.39 Dafoe similarly attempts to widen the scope of technological determinism by placing it as an endpoint on a spectrum, with social constructivism on the other end. The purpose of this spectrum is to create the space for engagement with disciplines that heavily emphasize power dynamics, including military affairs and business in what he terms “military-economic adaptationism.”40 Unfortunately, both Fino and Dafoe concede that attributing agency and causality to technological developments are best “conducted after the fact”41 or “on longer timescales,” respectively.42 AI governance cannot benefit from such hindsight, as it is fundamentally a question of how to project and adapt to forces of ongoing change. For governance, this inertia places military organizations at odds with the responsiveness required to guide responsible technology governance frameworks. Our aim is not to reconcile these differences in this chapter, but rather to highlight how they frame one current governance challenge for military stakeholders such as NATO: how can they engage with the socio-technical foundations in RRI frameworks to shape, adapt to, and respond to technology-accelerated changes, while simultaneously pursuing their traditional aims of adopting technology to deter and defend? On this note, it is worth mentioning that NATO itself has historically convened scholars from both STS and military innovation backgrounds to understand socio-technical changes to their operating environment.43 The Alliance also takes socio-technical factors into account in its S&T work on emerging technologies—including human–systems integration, technology monitoring, and forecasting work.44 This interest in socio-technical systems relating to effectiveness suggests scope for the Alliance to leverage technology governance as an instrument of its influence, as picked up in the next section. NATO’s Mechanisms to Govern AI NATO’s increasing interest in EDTs introduces the need to consider how governance priorities can help reinforce the Alliance’s influence. The STS and military innovation literature provide the theoretical foundations for NATO’s stewardship of AI as they place attention on “the role that institutions play in shaping technological trajectories.”45 As AI development continues, the actions that NATO and its members take will have important implications for their capacity to adopt, respond to, and shape their future operating environment. Particularly for democracies, this confers to military stakeholders a dual responsibility to prevent and manage risks, as well as to proactively shape their approach to technological development anchored in democratic values and security. As a multinational alliance with an incentive to drive cooperation and alignment, NATO is situated to define and operationalize norms, as well as promote standards that help shape the contours of future military effectiveness and technological competition. In a RRI framework, not only is this an institutional role, but it also becomes an institutional responsibility. To apply this responsibility to NATO’s stewardship of AI, the institutional interplay between technology, structure, and concepts is a form of socio-technical system with important implications for AI governance because they link the ways that an institution uses its power to adopt and shape AI trajectory to its respective ends. Already, several mechanisms are built into military bureaucracies to ensure that technology is adopted in alignment with responsible engineering practices and responsible state behavior.46 The Alliance is organized to harmonize between Allies so that their contributions enhance military effectiveness and political cohesion between like-minded democracies. We argue that these effectiveness-centric mechanisms likewise empower NATO to exert its influence in technology governance. More specifically, this entails the Alliance helping steward technological development for a more predictable strategic environment and enhanced democratic clout around the exploitation of technology reinforcing rule of law. For NATO, we focus on strategic and policy planning, as well as standards and certification because they reflect the Alliance’s particular strengths and interests in S&T. These practices are relevant to governance insofar as they exemplify an institution’s power to shape the trajectory of technological development—but this selection is by no means exhaustive.47 Instead, our aim is to explore how these mechanisms are operationalized at the Alliance level. In this vein, Table 69.1 dissects the role that its various bodies play in managing technology, promulgating and operationalizing standards, and leading change through policy. The role of NATO in this equation is largely shaped by its members’ own approaches to technology, and member-state-driven processes are complemented by “policy entrepreneurs” and technical experts in the International Staff and related bodies.48 Table 69.1 does not list the ways that AI affects the various functions of NATO, but rather spotlights the entities that together operationalize AI governance through cumulative processes on policy and standardization. Strategic and policy planning NATO structures around strategic and policy planning both set Allied ambitions and priorities and have the competency to implement them through its many consultative bodies, coordination formats, and albeit to a lesser extent, technology foresight capacities. NATO has facilitative power among Allies, both for defense planning and for the conduct of operations. A cornerstone in modern architecture of international security is coalition warfare—or, more broadly, joint operations. Working with military partners has become a critical feature of modern security policy, where there is more power in enhancing numbers, but also in having allies that lend political and practical legitimacy to deterrence and operations.49 NATO is vital to that effort for many reasons, but also because NATO’s facilitative power is significant to promote coordination and cooperation. Simply put, partners and allies are a necessary feature of modern military behavior, and strategic and policy planning are necessary functions to encourage and underpin cohesion in alliance settings. This is important for AI governance because the nature of AI poses new strategic challenges and will require multilateral approaches and some degree of cohesion to effectively incorporate RRI frameworks in policy planning. As such, the necessity of working with security partners extends to the AI-policy frontier. A number of NATO entities carry out strategic and policy planning, recognizing the importance of policy alignment to sustain political strength and military effectiveness. As relates to S&T, allies’ representations to NATO, defense ministries, and policy entrepreneurs from the relevant entities summarized in Table 69.1 support and negotiate how the Alliance approaches EDTs. NATO’s strategic documentation and forward-looking policy analysis incorporates hints of technological determinism, including noting how technological change inevitably shapes the future strategic and operating environment. Further, the connections between technology and competitive advantage over adversaries and competitors are embodied in the Alliance’s desire to maintain its “technological edge” as the “foundation upon which NATO’s ability to deter and defend against potential threats ultimately rests.”50 This places technology squarely within NATO’s core purpose of deterrence and defense—and while this signals NATO’s express commitment to technology through these channels, this reliance on technology also obscures whether NATO’s governance capacity will be adaptive, anticipatory, or participatory. This position of technological determinism may result in more limitations for AI governance. Standards and certification To maintain its relevance in a security architecture increasingly concerned with the way that technology shifts power dynamics and scales threats to international security, NATO has an incentive to foster cooperation, promote standards of practice, and incentivize Allied AI harmonization. It is strategically salient to facilitate a dialogue and engagement among Allies on AI, but it is practically important to use NATO’s position to facilitate Allied cooperation regarding standards to project the Alliance’s ability to interoperate in future operations. NATO standards aim to enhance interoperability among partners and successful implementation of strategy. More specifically, standards and certification are used to establish and implement requirements aligned with safe development and responsible use of technology. In addition to purely technical standards, NATO has operational standards that specify “conceptual, organizational or methodological requirements to enable materiel, installations, organizations or forces to fulfil their functions or missions.”51 In line with the definitions from STS and military innovation scholarship, standards can thus be seen as a mechanism to translate responsibility-derived state and organizational AI policy into actionable functions. In fact, NATO has set certain standards for the Allies and these standards subsequently become the norm. Within NATO, it is the NATO Standardization Office (NSO) that coordinates thousands of experts to align technological development with military requirements that can help enhance effectiveness, interoperability, and cohesion.52 While the NSO is primarily responsible for setting standards, other NATO entities—including in the NATO Science and Technology Organization (STO)—play important roles in implementing them and coordinating between national approaches.53 Certification frameworks and the promulgation of best practices can similarly help incentivize the transposition of RRI into military organizations, even if standardization is by no means a purely military governance tool. Both mechanisms, strategic policy planning and standards and certification, provide options for NATO to participate in AI governance regimes focusing on international security. NATO’s operationalization of these tools may hold important implications while implementing successful AI governmental regimes for Allies and other defense stakeholders. In the next section, we consider each mechanism within foundational issues, or pillars, to illustrate NATO’s role in AI governance. NATO and Technological Change: Three Pillars of AI Governance This section considers three pillars where NATO has procedures and competency to operationalize AI governance through both mechanisms of policy alignment and standards, and enhance security in the international environment. The pillars reflect foundational issue areas constitutive of governance but are also issue areas where previous scholars have cautioned as particularly challenging in the AI governance space. The three pillars—(1) ethics and values, (2) legal norms, and (3) safety and security—are meant to illustrate three conditions for NATO to facilitate policy and standards harmonization. Importantly, these pillars are not exhaustive areas in which NATO will need to consider governance structures to responsibly implement AI technology, but rather highlight particular issues that researchers and analysts acknowledge as significant hurdles in navigating AI governance (see Table 69.2).54 The first pillar considers NATO’s role in the evolution of ethical and values-driven AI. One ongoing debate regarding AI as a military technology is the ethical implications and baseline values the Allies, and others, want infused in the development and adoption of AI. The Allies themselves lack uniform consensus on numerous, substantial ethical questions on the use of AI, as most clearly seen in the adjacent area of the ethics of autonomy in weapons systems including lethal autonomous weapon systems (LAWS). In this discussion, we spotlight NATO’s role in facilitating and shaping ethical harmonization as an operational requirement to ensure successful future missions. The second pillar examines legal norms as a domain wherein legal uncertainty regarding AI has tangible implications for Allied legal interoperability, a subset of larger coalition interoperability. Thus far, the legal debate regarding AI has been largely fixed on the issue of a treaty banning the use of LAWS. In this section, we advocate for a more nuanced legal picture in which NATO can facilitate legal coordination and tackle some of the foundational legal issues which will prevent successful legal interoperability in future operations. The third pillar identifies safety and security of AI systems as prerequisite to trustworthy and responsible AI in any context, but especially so for the conduct of military activity. At the NATO level, Allied forces must ensure their systems interoperate safely and predictably both to ensure effective command and control (C2) internally, and to prevent disruptions from attacks. It is a foundational facet of coordination that shows the overlap between NATO interests in military effectiveness and incentivization for responsible innovation.

### Impact – Democracy Good

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

MattKroenig 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—t**hat’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.

### Impact – Authoritarianism

#### 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.

### AT: Disease Turn

#### Authoritarian states are worse for disease control – no info sharing.

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.

#### Disease impact is minimal – Reject their fear-mongering

Orent 15—anthropologist and freelance science writer whose work has appeared in The Washington Post, The LA Times, The New Republic, Discover, and The American Prospect, instructor in science journalism at Emory [Wendy, “Ignore predictions of lethal pandemics and pay attention to what really matters” 1/3/2015, http://www.latimes.com/opinion/op-ed/la-oe-orent-pandemic-hysteria-20150104-story.html Accessed 8 July 2017]

Prophets of doom have been telling us for decades that a deadly new pandemic — of bird flu, of SARS or MERS coronavirus, and now of Ebola — is on its way. Why are we still listening? If you look back at the furor raised at many distinguished publications — Nature, Science, Scientific American, National Geographic — back in, say, 2005, about a potential bird flu (H5N1) pandemic, you wonder what planet they were on. Nature ran a special section titled — “Avian flu: Are we ready?” — that began, ominously, with the words “Trouble is brewing in the East” and went on to present a mock aftermath report detailing catastrophic civil breakdown. Robert Webster, a famous influenza virologist, told ABC News in 2006 that “society just can't accept the idea that 50% of the population could die. And I think we have to face that possibility.” Public health expert Michael T. Osterholm of the University of Minnesota, at a meeting in Washington of scientists brought together by the Institute of Medicine, warned in 2005 that a post-pandemic commission, like the post-9/11 commission, could hold “many scientists … accountable to that commission for what we did or didn't do to prevent a pandemic.” He also predicted that we could be facing “three years of a given hell” as the world struggled to right itself after the deadly pandemic. And Laurie Garrett, author of what must be the urtext for pandemic predictions, her 1994 book “The Coming Plague,” intoned in Foreign Affairs that “in short, doom may loom.” Although she followed that with “But note the may,” the article went on to paint a terrifying picture of the avian flu threat nonetheless. And such hysteria still goes on: Whether it's over the MERS coronavirus, a whole alphabet of chicken flu viruses, a real but not very deadly influenza pandemic in 2009, or a kerfuffle like the one in 2012 over a scientist-crafted ferret flu that also was supposed to be a pandemic threat. Along the way, virologist Nathan Wolfe published “The Viral Storm: the Dawn of a New Pandemic Age,” and David Quammen warned in his gripping “Spillover” that some new animal plague could arise from the jungle and sweep across the world. And now there's Ebola. Osterholm, in a widely read op-ed in the New York Times in September, wrote about the possibility that scientists were afraid to mention publicly the danger they discuss privately: that Ebola “could mutate to become transmissible through the air.” “The Ebola epidemic in West Africa has the potential to alter history as much as any plague has ever done,” he wrote. And Garrett wrote in Foreign Policy, “Attention, World: You just don't get it.” She went on to say, “Wake up, fools,” because we should be more frightened of a potential scenario like the one in the movie “Contagion,” in which a lethal, fictitious pandemic scours the world, nearly destroying civilization. But there were fewer takers this time. Osterholm's claims about Ebola going airborne were discounted by serious scientists, and Garrett seemingly retracted her earlier hysteria about Ebola by claiming that, after all, evolution made such spread unlikely. The scientific world has changed since 2005. Now, most scientists understand that there are significant physical and evolutionary barriers to a blood and fluid-borne virus developing airborne transmission, as Garrett has acknowledged. Though Ebola virus has been detected in human alveolar cells, as Vincent Racaniello, virologist at Columbia University, explained to me, that doesn't mean it can replicate in the airways enough to allow transmission. “Maybe … the virus can get in, but can't get out. Like a roach motel,” wrote Racaniello in an email. H5N1, we understand now, never went airborne because it attached only to cell receptors located deep in human lungs, and could not, therefore, be coughed or sneezed out. SARS, or severe acute respiratory syndrome, caused local outbreaks after multiple introductions via air travel but spread only sluggishly and mostly in hospitals. Breaking its chains of transmission ended the outbreak globally. There probably will always be significant barriers preventing the easy adaptation of an animal disease to the human species. Furthermore, Racaniello insists that there are no recorded instances of viruses that have adapted to humans, changing the way they are spread. So we need to stop listening to the doomsayers, and we need to do it now. Predictions of lethal pandemics have — since the swine flu fiasco of 1976, when President Ford vowed to vaccinate “every man, woman and child in the United States” — always been wrong. Fear-mongering wastes our time and our emotions and diverts resources from where they should be directed — in the case of Ebola, to the ongoing tragedy in West Africa. Americans have all but forgotten about Ebola now, because most people realize it isn't coming to a school or a shopping mall near you. But Sierra Leoneans and Liberians go on dying.

## Solvency

### 2ac – Must Read

#### NATO key, US key, Military Logistics & Sustainment Key, Say Yes, Spills Over

Konaev & Chahal ’21 (Margarita Konaev is a research fellow with CSET, where Husanjot Chahal is a research analyst. "The Path of Least Resistance Multinational Collaboration on AI for Military Logistics and Sustainment" April, Center for Security and Emerging Technology, Georgetown University, https://cset.georgetown.edu/wp-content/uploads/CSET-Path-of-Least-Resistance.pdf)

Pathways to Collaboration The United States and its allies face powerful technical, political, and strategic reasons to pursue and deepen collaboration on AI applications for logistics and sustainment. Whether working within existing frameworks or building new partnerships, there are multiple pathways for collaboration. The final NSCAI report, for example, offers a comprehensive list of ongoing multilateral efforts on AI and associated technologies as well as security alliances and partnerships, some of which could serve as a forum for allies to work together on AI-enabled logistics.64 Below, we recommend four options for allies to explore depending on their interests and capabilities. 1. The United States and its allies should establish joint standards and protocols for the safe and secure sharing, pooling, and storage of nonsensitive datasets relevant to AI applications for logistics and sustainment. Data relevant to AI-enabled logistics and sustainment includes data on licensing, maintenance personnel, and repair schedules for predictive maintenance; video and navigation data from ground and aerial semiautonomous and autonomous resupply systems and convoys; data supporting maritime awareness and global shipping, and many other tasks and functions. Considering that data is the foundation of AI/ML-based applications, the United States and its allies will have to agree on standards regulating data sharing, storage, and analysis to ensure privacy, fairness, security, and respect for civil liberties. Identifying the governmental body to lead standardization efforts is a key step. Within the Department of Defense, for example, the responsibility for “the use and implementation of standardization” rests with the Defense Standardization Program Office International Standardization Program.65 Another option is to build on the NSCAI recommendation that the U.S. National Institute of Standards and Technology lead efforts to “promote international standardization in areas that further U.S. and allies’ national security and defense interests in the appropriate and responsible use of AI.”66 Allies will also need to decide on the scope of such standardization efforts. One pathway for alliance-wide collaboration is through NATO standardization agreements that facilitate interoperability, in part by ensuring the commonality of doctrine, procedures or equipment used and compatibility between allies’ products, processes, and services.67 That said, the lead body and institutional configuration for standardization efforts and data partnerships related to AI-enabled logistics and sustainment can and should vary depending on allies’ needs, interests, and capabilities. 2. The United States and its allies should collaborate on R&D initiatives related to AI for logistics and sustainment. When taken together, the R&D spending of the United States and just six like-minded nations—France, Germany, India, Japan, South Korea, and the United Kingdom—account for more than 50 percent of global R&D investment.68 This is a massive capacity for innovation. And when coupled with the shared interest in AI solutions for logistics and sustainment, there are many opportunities for collaborative R&D projects related to these technologies. One option is to add joint research and development initiatives related to AI for logistics and sustainment to the agenda of earlystage collaborative efforts like the JAIC’s AI Partnership for Defense. Future meetings coordinated by this partnership could serve as a launchpad for R&D projects that include any number of the interested member states. Another option is to expand existing bilateral and multilateral R&D collaborations to include projects related to AI applications for logistics and sustainment. The Technical Cooperation Program, for example, is a collaboration forum for defense research and development activities among Australia, Canada, New Zealand, the United Kingdom, and the United States.69 3. The United States and its allies should promote multinational private-public partnerships to advance research, development, procurement and fielding of AIenabled logistics and sustainment technologies. The United States and its allies are home to many small, midsized, and large-scale private companies with international presence and expertise in AI solutions for financial and business processes, healthcare, autonomous vehicle technology, maintenance management, and other areas relevant to logistics and sustainment. Private companies are at the forefront of innovation in AI, and there are great opportunities to leverage their expertise and commercial interests in defense to establish new and strengthen existing multinational private-public partnerships with a focus on AI applications for logistics and sustainment. The United States could work with allies on a bilateral basis; for example, building on Germany or South Korea’s competitive edge in autonomous vehicles technology to explore opportunities for public-private partnership for innovation in autonomous resupply technologies. There is also the option of working with and through regional bodies like the EU to support existing initiatives and public-private partnerships located in allied countries. 70 Another pathway suggested by experts at the Center for a New American Security in their report on building an alliance innovation base is to “launch a cross-national platform to build new companies” focused on national security technologies.71 4. The United States and its allies should include AI-enabled logistics and sustainment technologies and capabilities in joint military exercises. As AI-enabled technologies become more commonplace, it is vital to include them in joint multinational military exercises.72 From simulations and computer assisted command post exercises to major field exercises that include combined arms live-fire maneuvers integrating air, naval, marine, land, and cyber forces as well as civilian elements, multinational military exercises help forge personal and professional partnerships between allies, ensure doctrinal and technical interoperability, and strengthen readiness.73 Multinational logistic support is different from unilateral logistic support. Thus, if allies expect to use AI-enabled logistic and sustainment technologies in multinational missions, they would benefit from experimenting and training to do so together. Incorporating AI-enabled technologies into joint military exercises will allow allies to test and assess the technologies’ performance and viability in uncontrolled and dynamic environments— conditions in which AI systems are known to be brittle and vulnerable to adversarial attacks. Utilizing AI-enabled logistical elements and functions in joint exercises can also help allied militaries collect feedback from users and assess compatibility between the new technologies and existing concepts of operations, tactics, techniques, and procedures. User feedback can serve to improve the technology, while lessons learned about the ways in which new technologies fit with operational doctrine can inform necessary adjustments, ultimately, strengthening interoperability and readiness. Moreover, including AI-enabled logistics and sustainment technologies and capabilities in military exercises can help build trust between human operators and intelligent technologies. The issue of trust in human-machine teaming is particularly consequential in the context of multinational coalition because people from different countries can differ in their attitudes toward technology which in turn could affect interoperability, military effectiveness, and mission success as a whole.74 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 AI-enabled 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 missions.

### S – Cooperation Good

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

Franke ’21, (Ulrike Esther Franke, senior policy fellow at the European Council on Foreign Relations, PhD in International Relations from the University of Oxford. “ARTIFICIAL DIVIDE: HOW EUROPE AND AMERICA COULD CLASH OVER AI,” ECRF, January 2021, <https://ecfr.eu/wp-content/uploads/Artificial-divide-How-Europe-and-America-could-clash-over-AI.pdf>)

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.

#### The US must take the lead on AI and set its own international rules to uphold global human rights, democracy, and to mitigate future risks of AI.

**Imbrie et al. ‘20** (Andrew Imbrie, Senior Fellow at Georgetown's Center for Security and Emerging Technology; Ryan Fedasiuk, Research Analyst at Georgetown's Center for Security and Emerging Technology; Catherine Aiken, Director of Data Science and Research at Georgetown's Center for Security and Emerging Technology; Tarun Chhabra, nonresident fellow with the Center for Security, Strategy, and Technology at the Brookings Institution; Husanjot Chahal, Research Analyst at Georgetown University's Center for Security and Emerging Technology; February 2022; “HOW THE UNITED STATES AND ITS ALLIES CAN DELIVER A DEMOCRATIC WAY OF AI”; CSET; <https://cset.georgetown.edu/publication/agile-alliances/)//akg>

The following 10 initiatives provide a roadmap for how the United States and its allies can defend against threats, network to seize opportunities, and project influence to safeguard democracy in the age of AI. Initiative 9: Shape global norms and standards for AI. 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. Optimal Partners: Canada, United Kingdom, Ireland, Australia, Singapore, and Japan Multilateral Fora: EU, OECD, International Organization for Standardization and International Electrotechnical Commission Joint Technical Committee 1 Sub Committee 42 – Artificial Intelligence, WTO, 3GPP, NATO-EU joint initiative on standards for emerging technologies Criteria for Partnership: To lead the global discussion on AI safety and ethics, the United States will need to build a coalition of like-minded, influential countries from which it can listen and learn and with whom it can shape norms and standards. Ideal partners will be countries that host active and engaged civil societies, who have historically aligned with liberal democratic values and U.S. policy priorities, and who most actively collaborate internationally to develop AI norms and standards. Allies that more frequently use information and communication technologies, issue governance documents about AI, and host robust public sector discussions about AI and image recognition are optimal partners for shaping global norms, standards, and best practices around these technologies. For one measure of technology use, we included the World Economic Forum’s Government Usage of ICT index, as well as a count of national AI governance documents provided by Nesta.88 We also measured commitment to a democratic way of AI by canvassing national AI strategies for mentions of “principles,” “norms,” “standards,” and “safety.” To measure international clout and diplomatic capacity, we captured the number of diplomatic posts each country operates worldwide, as well as their ranks on the Soft Power 30 Index.89 Finally, we recorded countries’ demonstrated willingness to ban technology imports from Huawei Technologies as a proxy for their willingness to work with the United States.90 Other considerations and caveats: The United States will need to expand cooperation beyond the aforementioned countries to promote liberal democratic norms and standards for AI. Sweden and New Zealand were among the top-scoring countries for this initiative. As the world’s largest democracy, India is also an important partner in this effort. Policymakers will need to weigh additional considerations: countries that generate a high quantity of policy documents about AI may not make for optimal partners if these documents do not align with U.S. values and policy priorities. What’s more, many national guidelines mention or touch on AI but are not directly related to AI, and data is not widely available for non-Anglophone countries.

#### NATO standardization and info sharing solve – key to manage Russian threat

Jankowski 21 [Dominik P. Jankowski is a security policy expert, diplomat, think-tanker and social media aficionado. Currently he serves as Head of OSCE and Eastern Security Unit at the Ministry of Foreign Affairs of the Republic of Poland. Previously he served as Chief Specialist for Crisis Management at the Ministry of Foreign Affairs (2014-2016), Expert Analyst and Head of the International Analyses Division at the National Security Bureau of the Republic of Poland (2010-2014), Senior Expert at the J5-Strategic Planning Directorate of the General Staff of the Polish Armed Forces (2009-2010) as well as foreign policy expert at the President Aleksander Kwasniewski “Amicus Europae” Foundation (2007-2010). *NATO in Era of Unpeace: Defending Against Known Unknowns.* “NATO and the Emerging and Disruptive Technologies Challenge.” Pp 99-101. March 19, 2021. Lublin Publications, https://ies.lublin.pl/wp-content/uploads/2021/03/nato-in-the-era-of-unpeace\_calosc-1.pdf#page=82]//PJ

Conclusions and Recommendations While the suggestion that EDTs will enable a new class of weapons that will modify the strategic landscape remains to be realised, a number of unresolved security puzzles underlying the emergence of these new technology areas have implications for NATO. As one looks to the future, new adversaries and new science and technology will emerge. The extent to which these EDTs may exacerbate or mitigate the global security and governance challenges that Russia currently poses to NATO Allies will remain an integral question as policy-makers navigate the complex global environment. NATO is a natural forum for deliberations about EDTs, especially in a transatlantic context. It also has vast experience, going back to the Cold War, in working towards standardisation and interoperability among Allies. However, the results achieved have been mixed, which underscores the challenges the Alliance now faces – there are not only 30 Allies with disparate levels of capability, but also a backdrop of rapid technological advances where some of its competitors and adversaries may hold significant advantages. In this context, NATO should concentrate on four core issues with regard to EDTs. First, as Andrea Gilli emphasizes, the Alliance should start a process on “NATO-mation.”29 In fact, the Alliance should serve as a primary transatlantic coordinating institution for information-sharing and cooperation between Allies on the security dimension of EDTs. NATO has an important role to play in the development of a common strategy based on an Alliance-wide EDTs threat assessment and an analysis of opportunities. Therefore, EDTs can serve as a unifying element for NATO’s work on future policies. Second, NATO will need partners on its path towards achieving a comprehensive implementation strategy on EDTs. This will require connection with the private sector early and often, clearly communicating NATO’s priorities and requirements while providing accessible opportunities for industry, including non-traditional ones. Much of the innovative work being undertaken in the commercial sector is being carried out by companies that have never worked in the defence realm or have no wish to do so. Therefore, building new partnerships at NATO with the private sector will enable the Alliance to increase awareness, share data, and creatively tap into experiences and knowledge. Moreover, NATO and the EU should initiate a strategic dialogue to address fundamental issues of tech governance and data sharing in order to overcome the transatlantic tech policy divide. Third, Allies should manage expectations and not overestimate the role of EDTs. EDTs are not a panacea to all of NATO’s problems, including the existing gaps in the still-needed conventional capabilities. Indeed, EDTs will not be a silver bullet to address NATO’s shortfalls. Therefore, Allies should first and foremost concentrate on two elements: overcoming the interoperability gap30 and revitalizing NATO’s once robust standardization programme.31

#### NATO cooperation creates a laboratory effect which spurs innovation.

Husain et al. 18(Amir Husain, August Cole, and Wendy R Anderson. CEO of Spark Cognition & Board of Adivisors for UT Austin’s Department of Computer Science & Member of Council on Foreign Affairs, Senior fellow of Scowcroft Center on Strategy and Security at the Atlantic Council & Fellow of Brute Krulak Center for Innovation and Creativity at Marine Corps University. " As Budget Polemic Drives Headlines, Do Not Lose Track of NATO’s Approach to AI". 07-27-2018. Royal United Services Institute. https://www.europarl.europa.eu/cmsdata/155282/WendyRAnderson\_RUSIArticle.pdf. 6-22-2022.)-cg

After European leaders faced renewed American pressure to more than double defense spending at NATO’s most recent summit, the budget debate is likely to become the headline-driving narrative about the Alliance’s future in the coming months on both sides of the Atlantic. Yet, what risks being eclipsed by the fiscal polemic is a critical conversation about how the 29 member states approach the one innovation with perhaps the greatest potential to up-end warfare and even NATO itself: artificial intelligence (AI). As an alliance whose potential is defined by the totality of its members, NATO faces a growing challenge in coordination and collaboration around military-relevant emerging technologies – perhaps even more than during the Cold War when there were fewer member states and a relatively unified threat from the Soviet Union and Warsaw Pact countries. Then, it was military innovation that led defense-relevant breakthroughs, the opposite of today’s private-sector driven innovation. AI research and implementation in particular is being led by companies, not governments. Now, and in the future, NATO’s missions will be increasingly dynamic and politically thorny – from policing migration to counternarcotics to strategic deterrence – because of the ‘algorithmic impact’ of increasingly capable social media bots, AI-created fake images and video, and even automated weapons platforms. Recent social media influence offers a preview. In Poland and the Baltic states, automated social media bots, which are a form of AI, produce ‘roughly 70% of all Russian messages about NATO’ according to a study last year from the NATO Strategic Communications Centre of Excellence. Underscoring the risks to come, Russia employed bots, or automated social media accounts, and exploited social media machine-learning algorithms during the 2016 election cycle to target US voters with ads and content designed to exacerbate partisan divides within NATO’s largest member. With a new NATO AI standard, NATO can employ AI in a manner that does more good than harm, operationally and bureaucratically speaking This can be expected to be amplified by states such as Russia, which harmonize highly disruptive propaganda and kinetic operations while committing to investments in military-relevant AI. As Russian President Vladimir Putin has said, ‘whoever becomes the leader in this sphere will become the ruler of the world’. Under President Xi Jinping, China’s ambitions are equally grand, with the state’s 2017 New Generation Artificial Intelligence Plan recognizing that China ‘must, looking at the world, take the development of AI to the national strategic level …’. As this is a larger global challenge, NATO is a perfect ‘laboratory’ for member states to find their way forward with AI by embracing commonality through the Alliance rather than going it alone. AI need not add to NATO’s recent challenges, fiscal or technological. Although individual European NATO members have promising government-and commercial-sector AI investment programs underpinned by national strategies, as the UK and France do, a standardized Alliance-driven approach ensures all members benefit from current and future breakthroughs.

#### Multilateral NATO cooperation necessary to facilitate framework around AI—that’s key for maintaining technical edge, ensuring accountability, and ethical usage.

Hill ‘20 [Steven Hill, served until February 2020 as Legal Adviser and Director of the Office of Legal Affairs (OLA) at the NATO International Staff, "AI's Impact on Multilateral Military Cooperation: Experience from NATO," 4-27-2020, American Journal of International Law | Cambridge Core, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ais-impact-on-multilateral-military-cooperation-experience-from-nato/3AEF22AA22550A10B75DD74A806D4D18]/lf

AI-based military applications present both opportunities and challenges for multinational military cooperation. This contribution takes stock of the state of discussions around AI-based military applications within the North Atlantic Treaty Organization (NATO). While there have been a number of recent developments in national AI strategies and policies, discussions at the NATO level are still in early phases, and there is no agreed NATO policy in this area. Further multilateral work is needed if like-minded states such as NATO Allies and partners are to head off the serious risk that disagreements about these technologies might hamper effective multilateral military cooperation. This essay first frames the overall strategic context within which discussions related to AI at NATO take place. Perceptions of security threats are shifting as a result of the rise of great power competition. At the same time, the AI policies of some individual Allies are rapidly evolving. The essay then describes the publicly-accessible work that has taken place within NATO on AI issues. It uses two potential military applications of AI that are likely to be of interest in a NATO context, as well as some positive and negative elements associated with them. Finally, the essay suggests the need for continued multilateral dialogue on military use of AI. NATO is an alliance of thirty states that has collective defense as one of its three core tasks.1 Part of NATO’s identity is as “an alliance that constantly modernises and adapts to new threats and challenges,”2 including those arising from the development of new technologies. As Allied Heads of State and Government put it at their meeting in December 2019 in London, “To stay secure, we must look to the future together. We are addressing the breadth and scale of new technologies to maintain our technological edge, while preserving our values and norms.”3 These two short sentences contain at least four different ideas that shed light on NATO’s strategic approach to AI. First, they emphasize maintaining “our” technical edge. This could be interpreted as referring to the collective advantage that NATO Allies enjoy or to the advantage that individual member states have. Second, the emphasis on maintaining an edge hints at the growing importance of great-power competition in NATO’s strategic thinking, especially with regard to China. The Alliance increasingly has turned its attention to China, with NATO leaders adopting historic language at the London Summit about the “opportunities and challenges” posed by China.4 Technological competition, including in the AI field, where China has made major advances, is one of these areas. Third, the statement refers to the need to “preserv[e] our values and norms” while dealing with the new technology. While not going into detail about what those values and norms are, this language flags the importance of legal and ethical considerations in working together. Finally, the statement has an express reference to the need for multilateral cooperation in this space going forward: “we must look to the future together.” Another element of the strategic context is the rapid proliferation of national military AI strategies adopted by individual NATO Allies. Many of these strategies explicitly include legal and ethical components. For example, France’s recent strategy on AI and defense sets forth three major principles: (1) respect for international law; (2) the presence sufficient human control; and (3) ensuring responsibility of human command. France is also working to create a defense-focused ministerial ethics committee whose purpose will be to discuss the implications of emerging technologies in the defense field.5 The 2018 German AI strategy—which is general in scope, not specific to the defense sector—refers to the need to “integrat[e] AI in society in ethical, legal, cultural and institutional terms in the context of a broad societal dialogue and active political measures.”6 In the United States, the Department of Defense recently adopted five principles that the Defense Innovation Board proposed to govern the development of AI systems in defense, emphasizing that such development must be: (1) responsible; (2) equitable; (3) traceable; (4) reliable; and (5) governable.7 While these strategies use some of the same categories of terms and thus appear to speak the same language, it is not clear to what extent states would agree about how to apply such principles in the context of a specific military use of AI. While these strategies are developed to govern work at the national level, they also tend to refer—if only in general terms—to the need for multilateral cooperation. The U.S. Department of Defense’s Joint Artificial Intelligence Center, for example, articulated as one of the pillars of its strategic approach “evolving our crucial international alliances and partnerships abroad. An extended network of mutually beneficial alliances and partnerships provides a durable means of overcoming global AI challenges, deterring aggression, and supporting stability through cooperation.”8 While the European Commission’s February 2020 AI White Paper excludes military AI from its scope,9 a food-for-thought paper on AI developed during the 2019 Finnish presidency of the European Union emphasizes the importance of cooperation with partners, including as part of the increasing trend toward EU-NATO cooperation.10 If NATO Allies must look to the future of new technologies together and if national strategies are calling for more international cooperation, it is worth asking what they have done together to date. Allied Command Transformation (ACT), one of NATO’s two strategic commands,11 has played a leading role in NATO’s work on innovation and disruptive technologies, including AI. In October 2019, for example, ACT organized an informal workshop with NATO ambassadors and military representatives.12 The focus of the event was “the Alliance’s efforts to leverage the power of data science, machine learning and other new technologies to improve its decisionmaking.”13 This event followed up on a similar informal workshop held in March 2018 designed to highlight the broader impact of the development of disruptive technologies on the Alliance.14 One take-away from this informal discussion was that allies may wish to discuss some of the legal implications of this emerging technology in a multilateral forum such as NATO. On the level of policy documents, NATO has developed an “Emerging and Disruptive Technologies Roadmap” that is meant to guide future Alliance work in this area. As ACT describes it, the Roadmap “uses a bottom-up approach to conduct rapid and tangible demonstrations in realistic operational conditions in order to understand the potential of Emerging and Disruptive Technologies from both the opportunity and threat standpoints and to set the conditions to use them within NATO and its Member Nations.”15 This could include drawing out some commonly accepted legal and ethical principles surrounding the military use of AI such as respect for international law, the need to keep humans in the loop, and the importance of clear accountability. More broadly, NATO is actively working to develop a data policy, specifically to put in place standards relating to the oversight of multinational pooling and sharing of data.16 Finally, in terms of training and exercises, NATO is also now regularly integrating new technology in its exercises, especially in the area of humanitarian assistance. For example, a NATO disaster response exercise held in Serbia in October 2018 successfully incorporated disaster relief tools powered by artificial intelligence such as the processing of aerial images of the simulated disaster site in order to identify victims more quickly.17

### S – NATO Says Yes

#### Allies will agree because alliance commitments – AI cooperation sovles and US is key.

Greenberg ‘20(Erik Lin-Greenberg, , “Article Title,” Journal/Magazine/etc, “Allies and artificial intelligence: Obstacles to operations and decision making”, Texas National Security Review, 3(2), 56–76, March 05 2020, https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/)-amc

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](https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/" \l "_ftn133) 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](https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/" \l "_ftn134) A state’s successful development of AI can therefore increase its voice and sway within complex multinational institutions.

#### NATO wants AI reg

Kirdemir 19(Can Kasapoğlu, Bariş Kirdemir. Director of Security and Defense Studies at EDAM and Eisenhower fellow at NATO defense college."Artificial Intelligence and the Future of Conflict". 11-28-2019. Carnegie Europe. https://carnegieeurope.eu/2019/11/28/artificial-intelligence-and-future-of-conflict-pub-80421. 6-22-2022.)

In recent years, European lawmakers have been actively seeking regulatory action amid emerging digital threats, data-privacy issues, and hostile influence campaigns. European policymakers often emphasize protecting core values, regulating big tech, and preventing malign actors from using AI and accompanying technologies to target Western political institutions, public safety, and individuals. NATO would benefit from a convergence of transatlantic regulatory and legislative frameworks to better steer the trajectory of the coming transformation.

#### NATO needs regulated AI - 3 reasons

Kirdemir 19(Can Kasapoğlu, Bariş Kirdemir. Director of Security and Defense Studies at EDAM and Eisenhower fellow at NATO defense college."Artificial Intelligence and the Future of Conflict". 11-28-2019. Carnegie Europe. https://carnegieeurope.eu/2019/11/28/artificial-intelligence-and-future-of-conflict-pub-80421. 6-22-2022.)

In 2018, a consortium of U.S. and European experts from industry, civil society, and research institutions published a report that outlined three areas of concern. The first is the digital security domain, in which the report warned of potential AI vulnerabilities that would allow adversaries to stage large-scale, diversified attacks on physical, human, and software targets. Second, in the physical security domain, the availability and weaponization of autonomous systems cause major challenges. Cyber and physical attacks on autonomous and self-driving systems and swarm attacks—coordinated assaults by many agents on multiple targets—are other potential threats. Third, there are significant risks to political security. AI-enabled surveillance, persuasion, deception, and social manipulation are threats that will intensify in the near future. New AI capabilities may strengthen authoritarian and discriminatory political behavior and undermine democracies’ ability to sustain truthful public debates. NATO nations need to develop an acceptable level of consensus in the governance of the AI transformation. Although this seems extremely difficult given the current state of political affairs, NATO exists for its member nations to come together and tackle these vital security challenges. AI is likely to cause large-scale economic and workforce shifts. Crucially, it is changing how geopolitical competition plays out. It will equip authoritarian states, some of which are competitors of NATO nations, with new oppressive and discriminatory tools. Besides, AI can offer increasingly smart autonomous weapons systems to states and nonstate actors. The transatlantic community will therefore have a full set of tasks on its plate, from observing how such dynamics develop in different regions to building international partnerships to ensure common interests and regulatory actions NATO would benefit from initiatives to prepare for, govern, and regulate AI-related policy priorities. From developing capabilities to building consensus on the challenges mentioned above, NATO needs new mechanisms to tackle emerging threats and continuously adapt to the dynamism of AI-led developments. Comprehensive collective initiatives are known to be effective in the cybersecurity field. The alliance should establish an AI task force to review policies and strategic issues. On the policy level, NATO should initiate a continuous and meaningful conversation among decisionmakers, industry, civil society, and the scientific research community. The alliance has a long way to go in developing algorithmic warfare capabilities and adopting an AI-enabled C4ISR structure. Because most innovations in AI and robotics come from outside the military-industrial complex, some studies have encouraged the alliance to cooperate closely with big tech or develop ties with promising start-ups. NATO must test its social-cognitive and digital-security vulnerabilities systematically. Ideally, red teaming—in which a group adopts an adversarial point of view to challenge an organization to improve its effectiveness or detect a major weakness—and experimentation efforts should cover both allied exercises and more isolated, peacetime activities to test defenses in national security apparatuses. Inputs from the interdisciplinary and multisectoral conversation, as well as continuous exercises, may provide significant information for new concepts.

#### Current AI development requires massive amounts of data mining and improvements to parallel systems (will be probably run-in conjunction with “NATO info/NATO collab key” warrants).

HR 21 (Harbor has over thirty years of experience working with clients on growth strategy and new business creation. At the core of our experience is a deep understanding of the technologies, markets and business characteristics—as well as the management and organizational challenges—that companies face when adopting and developing digital and smart systems) “Capturing the Value of AI” <https://harborresearch.com/capturing-the-value-of-ai/> July 21, 2021 // ZX

As networks continue to invade the “physical” world, traditionally unique components and interfaces between and among electronic as well as electro-mechanical elements are becoming more standardized. Product and service design is increasingly influenced by common components and sub-systems. Vertically defined, stand-alone products and application markets will increasingly become a part of a larger “horizontal” set of standards for hardware, software, communications and data. As it becomes easier to design and develop smarter more adaptive systems, competitive differentiation will shift away from unique product features towards how the product is actually used, how the product fosters interactions between and among users in a networked context, and, most importantly, how the data from the product will inform these new insights. Machine data from cyber-physical systems of the real physical world can offer extraordinary business advantages to the companies that understand how to organize that data and model the behavior of the physical world. The ability to develop models from sensor and machine datasets allows not only data patterns but a much higher order of intelligence to emerge. Widespread adoption of AI and machine learning systems is inevitable. But that doesn’t mean that every participant will automatically be shaking a money tree. Value and returns from AI/ML are playing a new game of hide-and-seek. They’re still there, but not where they used to be. If you keep looking in the old places…well, you know what’s going to happen. We think that the economic impact of AI/ML developments will recapitulate the tendency we’ve seen for decades in digital technology generally—less and less physical value, and more and more metaphysical value. Of course, digital computing has radically transformed human affairs. But so far that transformation has taken place entirely on the computer’s terms. Note that even the most remarkable recent achievements of AI and machine learning—autonomous driving, natural language processing, text generation, facial recognition, algorithm design and [vaccine discovery](https://harborresearch.com/covid-testing-at-the-speed-of-light/)—have occurred in domains of our physical environment that are subject to rigid sets of rules and laws. We’re in the third decade of the 21st century, and the question still remains, “How many engineers in white lab coats does it take to make AI valuable?” Rapid advancements in silicon, computing and networks are clearly forming the foundations for AI and machine learning capabilities to advance. But these systems, sophisticated as they are, are still in their early stages, and many intended use cases for AI can still be accomplished with more cost-effective traditional tools like basic regressions. It seems clear that [real business value from machine learning and AI](https://harborresearch.com/data-ai-drive-new-business-models/) will be realized unevenly across markets, applications and use cases. Possibly most important for the growth of AI is that multiple parallel technology developments are now increasingly reinforcing and accelerating one another. Cloud infrastructure resources are providing unprecedented computing scale. Mobile computing devices are extending the reach of computing. Embedded systems and IoT technology are connecting and integrating a broad array of physical and digital applications. And of course the signature achievement of the age of “big data,” the ability to capture and process massive amounts of [raw intelligence from the physical world](https://harborresearch.com/physical-gets-metaphysical/), has the potential to inform many new and diverse capabilities. Each of those technologies is powerful on its own, but creative combinations of them are what is most exciting. Human-connected devices and machine-connected IoT devices enable exponentially more data at the edge. The scale of core, infrastructural (cloud) computational capabilities enables us to capture and analyze all that information. And this in turn sets the stage for AI and machine learning tools to analyze and capture new insights. This new chapter is motivating tech developers and users to apply advanced neural nets and deep learning tools to their most intractable problems. Most companies believe that implementing advanced AI solutions will lead to significant efficiencies, growth and competitive differentiation. However, matching new tools to high value applications and use cases will challenge many industry participants. We all know that AI tools are trained on large data sets, but most people do not grasp that AI applications require thousands or even hundreds of thousands times more data than a human would need to solve an equivalent problem. If you examine applications where machine learning is successful, it quickly becomes apparent that they are in domains where acquiring lots of data is relatively easy—think facial or speech recognition, where technology developers have vast troves of data they can access. Data-driven apps are the core value creation mechanisms within the Smart Systems and the IoT. But the B2B world that comprises so much of the IoT doesn’t have the same unified sources or monolithic usage tracking and analytics that the consumer world utilizes to make money. Based on our consulting work, we estimate that B2B development projects lack as much as half the data needed to inform new application values and fulfill on artificial intelligence and machine learning opportunities. An additional challenge is the fact that most machine learning systems today run “narrow purpose” applications that can do only a single type of learning. Current neural networks cannot be trained to run multiple parallel applications, such as identifying images and playing video games, or predictively diagnosing machine failures and listening to and identifying music, all at the same time. Finally, the impacts of new AI tools will be higher and more straightforward to achieve where the user’s propensity to experiment with new tools and methods is also higher. AI and machine learning are being turbo charged. An explosion of AI/ML tools is lowering the barrier to entry to high-end data science. Historically, developing AI/ML applications and use cases involved data teams doing much “heavy lifting” to design and deploy complex custom models. Today, new data tools are gaining wider adoption. Standardized schemas for data ingestion and transformation are setting the stage for many more companies to incorporate AI/ML into their products.

#### Allies expressed almost unilateral interest in info-sharing and NATO acts as a foundation for interoperability, info-sharing, and data analysis.

Imbrey et al 20 (Andrew Imbrie is a Senior Fellow at Georgetown's Center for Security and Emerging Technology (CSET). He previously worked as a fellow at the Carnegie Endowment for International Peace and as a senior advisor to Visiting Distinguished Statesman Secretary John F. Kerry.) “HOW THE UNITED STATES AND ITS ALLIES CAN DELIVER A DEMOCRATIC WAY OF AI” Feb 2020 Edition [https://cset.georgetown.edu/wp-content/uploads/CSET-Agile-Alliances.pdf //](https://cset.georgetown.edu/wp-content/uploads/CSET-Agile-Alliances.pdf%20//) ZX

The Chinese government undertakes multiple, coordinated efforts to obtain sensitive information from U.S. AI researchers. Many of these pathways and access points for technology transfer are legal or extralegal and therefore poorly understood or monitored by Western intelligence agencies.28 Common vectors include technology transfer centers and forums, copyright infringement, and grant and funding opportunities for Chinese undergraduate, graduate, and post-doctoral researchers to study abroad and collaborate with foreign universities, research labs, and companies.29The United States could improve coordination with allies and partners to counter technology transfer in several ways. Strategic Initiatives 4 T 12 Center for Security and Emerging Technology surveyed country indicated interest in coordinating with the United States to prevent the transfer of sensitive technology. This initiative received the second highest level of agreement, just after coordinated AI norms and standards. Respondents from Japan, Australia, Italy, and France were particularly interested in collaboration around tech transfer policies. The United States should work with allied and partner governments to develop common standards for sharing, pooling, and storing non-sensitive, government-owned data sets. U.S. allies and partners are broadly open to non-sensitive data-sharing arrangements: Nearly 90 percent of officials indicated interest in sharing more data with the United States, and 75 percent cited specific non-sensitive data their country would be willing to share. More than half of responding countries indicated a willingness to share weather pattern data, epidemiological data for disease control, medical images for precision medicine, and video and navigation data from self-driving cars. This initiative may be among the most important for America’s European partners. An EU official noted that the EU would likely be willing to share quite a lot of data, provided rules are in place and enforced. The United States could partner with Singapore, Spain, Italy, and other NATO allies on a data-sharing initiative related to maritime domain awareness in the way that Indonesia, Malaysia, and Singapore, for example, share hydrographic data and cooperate to improve their anti-submarine warfare capabilities.52 NATO states that the maritime domain “is of strategic importance.” Its members could share militarily relevant datasets to improve maritime domain awareness in the Black Sea and other strategic locales.53 U.S. policymakers could also work with counterparts in allied and partner countries to develop common standards for data archival procedures, including standards for ensuring the data is labeled, stored, interoperable, and accessible.54 The U.S. Open Government Initiative began to lay the groundwork for common data standards as early as 2013, and the United States should promote similar practices among allies and partners.55 Such a collaborative approach would enable data flows and promote healthy data management among allies that could further propel the growth of AI. Optimal Partners: United Kingdom, Germany, Japan, France, the Netherlands, and New Zealand Multilateral Fora: NATO, the European Commission, Five Eyes, OECD, Association of Southeast Asian Nations (ASEAN) Criteria for Partnership: Optimal data-sharing partners would be countries that widely collect and publish data for public use, and countries where that data is stored and accessible by third parties.

### S – Coordination Key

#### The basis for regulation closer to conceptual than mechanical

Husain et al. 18(Amir Husain, August Cole, and Wendy R Anderson. CEO of Spark Cognition & Board of Adivisors for UT Austin’s Department of Computer Science & Member of Council on Foreign Affairs, Senior fellow of Scowcroft Center on Strategy and Security at the Atlantic Council & Fellow of Brute Krulak Center for Innovation and Creativity at Marine Corps University. " As Budget Polemic Drives Headlines, Do Not Lose Track of NATO’s Approach to AI". 07-27-2018. Royal United Services Institute. https://www.europarl.europa.eu/cmsdata/155282/WendyRAnderson\_RUSIArticle.pdf. 6-22-2022.)-cg

A new NATO standard for AI is not a set of measurements or technical specifications, as would be used in establishing, for example, a common calibre for small arms ammunition. This is the era of decentralised innovation and software-driven warfare, where accessible data confers strategic advantage and social media can be as tactically relevant as a light machine gun. This approach to a new NATO AI standard is more of a framework than a technical specification, but it is equally crucial for developing a common understanding and set of expectations about what kind of AI systems the Alliance can utilise. This approach is derived from the operational capabilities covered in the joint NATO operational planning framework. Each operational phase has distinct ways that AI can be most effectively used at an Alliance level. The next step would be the development of specific technical guidelines once an overarching common NATO approach is agreed to.

**Ethical AI development increase NATO interoperability – that props up democratic norms**

**van der Merwe ‘21** [Joanna van der Merwe holds an 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, 2-17-2021, accessed on 6-23-2022, CEPA, "NATO Leadership on Ethical AI is Key to Future Interoperability", https://cepa.org/nato-leadership-on-ethical-ai-is-key-to-future-interoperability/]//PJ

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: 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.

### S - Private Partnerships

#### Budget is directly relevant to NATO AI interoperability but independent companies allow realignment

Dufour 18(Martin Dufour. Former CWO of the Canadian Army and Reciever of the Eisenhower award. " Will artificial intelligence challenge NATO interoperability?". 12-10-2018. NATO Defense College. https://www.jstor.org/stable/pdf/resrep19838.pdf?refreqid=excelsior%3A3d8e2cb1e4b2742d7de11be85a7eedec&ab\_segments=&origin=&acceptTC=1. 6-24-2022.)-cg

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” 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”. This echoed a 2016 report from the Armament Industry European Research Group, which concluded that “a further boost in US defense technology could promote a wider US-Europe gap and the emergence of a two-tier alliance”. 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”. 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 artificial intelligence and autonomous technologies reveals that most of the innovations in the field occur outside the military-industrial complex. The GAFAs (Google, Amazon, Facebook, Apple) have steadily invested over the years to develop commercial applications for artificial intelligence, and one can find many other startup companies throughout the world. The data company CB Insights’ second annual AI 100 list identified the 100 most promising artificial 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”. NATO states should therefore strive to develop partnerships with such companies, identify promising applications, and start implementing them at once in their defense 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 fields, 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 conflict. These capabilities could offset complex hardware solutions and allow smaller nations to continue sharing the burden of military operations. This is the point made in a 2017 study titled Artificial Intelligence and the Future of Defense, according to which given its “algorithmic and non-defense specific essence…[artificial intelligence] is easier to jump in than is the case for many industrial-kinetic technologies [such as] building a sixth-generation jet fighter”. As such smaller, nimble nations have an opportunity to redefine how they do military development, and harness this key disruptive technology to start filling the growing capability gap between NATO countries.

### S – Legal Clarity

#### Plan builds trust by solidifying legal principles – coop solves

Hill ‘20 [Steven Hill, served until February 2020 as Legal Adviser and Director of the Office of Legal Affairs (OLA) at the NATO International Staff, "AI's Impact on Multilateral Military Cooperation: Experience from NATO," 4-27-2020, American Journal of International Law | Cambridge Core, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ais-impact-on-multilateral-military-cooperation-experience-from-nato/3AEF22AA22550A10B75DD74A806D4D18]/lf

Conclusion: The Need for Multinational Dialogue As noted above, the different national strategies refer to the need for legal and ethical frameworks. They also generally refer to the desirability of multilateral cooperation on AI. The limited work within NATO so far has also pointed to a willingness to take on these issues in a multinational setting. However, the reality is that these discussions have not yet taken off. There may be good reasons for this, including the ongoing nature of LAWS discussions in Geneva or the understandable reluctance—frequently encountered with respect to new technologies—to take positions that could constrain innovation or that could present a strategic disadvantage to those who abide by the rules. At the same time, the perception that there are unresolved legal or ethical issues hovering over military applications of AI clearly poses a risk to the use of this technology, including in a multilateral military setting. There is generally broad agreement among NATO allies that existing international law should apply to the military use of new technologies, including AI. However, a perception of lack of clarity on the rules of the game may lead to a lack of trust that might hamper multinational cooperation. In this regard, dialogue about legal and ethical frameworks can be an important means of building trust. Individual NATO Allies are in the midst of developing their own national strategies for military applications of AI. As noted above, while these strategies use some of the same vocabulary in calling for more clarity on the legal and ethical frameworks of military AI, there is a real risk of a lack of meeting of the minds about the substantive content of these frameworks. Consider but one of the issues that will arise: the potential scope of difference of views related to data ownership, sharing, and use.18 If data is “fuel” for AI, the question of who owns it and under what conditions it can be shared and used by others is of strategic importance. Despite the sense that like-minded countries will need to cooperate to develop their own sources of such “fuel,” there is no agreed transatlantic approach in policy and law on how to handle a wide range of data-related legal issues. Data sharing arrangements need to be in place beyond the limited, generally law enforcement-related sectors in which there are existing arrangements. There is considerable work to be done to create the necessary trust to develop mutually-agreed procedures that strike the balance between the many different equities involved in such an exchange of information. While most of these discussions on data take place outside of NATO, NATO does have some experience that could be relevant. For example, NATO already has in place mechanisms for the secure sharing of information that are based on trust built over the life of a seventy-year-old Alliance. NATO has recently built upon these practices to promote the sharing of evidence gathered in battlefield settings for use in the criminal prosecutions of foreign terrorist fighters.19 Achieving consensus agreement on these initiatives required a considerable amount of legal dialogue for Allies to find a pragmatic way forward, building on NATO’s tradition of “legal interoperability.”20 In the end, NATO’s early-days experience shows that in a multinational setting, it is important to understand AI-enabled military applications and to support their implementation in practical contexts. This requires open dialogue between Allies and other partners as well as with industry. NATO has the potential to play a unique role in this process

### Lots of Mechanisms

#### A coordinated AI effort between the US and its allies improves interoperability and increases security

**Imbrie et al. ‘20** (Andrew Imbrie, Senior Fellow at Georgetown's Center for Security and Emerging Technology; Ryan Fedasiuk, Research Analyst at Georgetown's Center for Security and Emerging Technology; Catherine Aiken, Director of Data Science and Research at Georgetown's Center for Security and Emerging Technology; Tarun Chhabra, nonresident fellow with the Center for Security, Strategy, and Technology at the Brookings Institution; Husanjot Chahal, Research Analyst at Georgetown University's Center for Security and Emerging Technology; February 2022; “HOW THE UNITED STATES AND ITS ALLIES CAN DELIVER A DEMOCRATIC WAY OF AI”; CSET; <https://cset.georgetown.edu/publication/agile-alliances/>)-amc

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 de- fenses 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 robust- ness, 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 capabil- ity 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-crit- ical systems. To ensure allies store and process data homogeneously, the United States and its allies should launch an accelerator fund for cloud computing. The United States and its allies could use this fund to more efficiently procure commercial cloud com- puting technology. The United States, United Kingdom, and Canada, for example, could agree to bid out a bulk purchase of cloud compute from major technology companies and distribute access to compute in the form of credits and publicly funded research. This initiative would ensure that democratic nations benefit from techniques in machine learning that require fewer inputs of real-world data but greater computational power to run simulations and self-play methods. Representa- tives from Japan, South Korea, the Czech Republic, Lithuania, and the EU each cited increased computing as an AI R&D priority, suggesting an area for aligning focus among allies. Parallel to this effort, the United States and its allies should launch a software development initiative. This initiative could take a page out of the U.S. Air Force’s Kessel Run project by pairing government-led teams with software developers from allied countries. Multinational teams could work together to build capabilities in agile software used in military systems that are part of joint exercises. Allies could also use AI to automatically create “translators” between systems and user interfac- es that are not yet fully interoperable. The United States and its NATO allies should consider partnering with existing frameworks like the AI4EU artificial intelligence test bed, which pools compute and data among EU countries.69 Optimal Partners: Canada, Australia, United Kingdom, Germany, Italy, and Japan Multilateral Fora: Five Eyes, NATO, NATO-EU (AI4EU) test bed partnership, U.S.-Japan-South Korea Trilateral Defense Cooperation, National Technology and Industrial Base (Australia, Canada, the United Kingdom, and the United States) Criteria for Partnership: The United States should improve technical interopera- bility with the countries that receive the most attention in U.S. global security opera- tions, interact the most with U.S. forces, and express the most concern about disjoint- ed technical requirements and capabilities.

#### An A3IC Agency is key---leadership in development of artificial intelligence by setting guidelines and procedures ensures cohesive development across NATO

Gilli 20 [Andrea Gilli December 2020 “’NATO-Mation’: Strategies for Leading in the Age of Artificial Intelligence” NATO Defense College Research Paper No.15 pp. 35-40 <https://www.ndc.nato.int/download/downloads.php?icode=671>] -os-

Championing innovation: artificial intelligence, integration and the implementation-enabling centre (A3IC) While innovation is often treated and discussed as an outcome, it is in fact also a process whereby champions – whether individuals or organizations – promote and implement changes leading to performance, mission or operational improvement.116 Within NATO, many stakeholders have an inherent interest in AI and in promoting the AI agenda. However, there is no clear “champion” whose goal is to steer the Alliance’s approach to adopting the technology, promoting the necessary reform, and devising the best practices for its employment. For this reason, the process of “NATO-mation” could benefit significantly from a centre specifically intended to serve this goal – tentatively referred to here as an Artificial Intelligence, Integration and Implementation-Enabling Centre (A3IC). Such a centre could lead adoption of AI for the Alliance, support Allies in their own adoption strategies, and connect the relevant offices and institutions at both the national and NATO levels. With a focus on training and interoperability, an AI champion for NATO could ensure that the Alliance treats innovation as an ongoing process and disseminates successful outcomes. The innovation process often requires a person or an organization mentoring, supervising, advocating and protecting innovations and innovators. Having an innovation champion is important to promote those micro-changes that often permit the successful adoption of an innovation: this is achieved by aligning the interests of all the individuals involved with the overall goal, so that resistance, opposition and sometimes even boycotting are minimized and addressed.117 While the buzzword “innovation” is generally perceived favourably, resistance often emerges because of cultural barriers such as opposition to change, sociological factors such as group identity and concern for loss of status, organizational dynamics such as career advancement being hindered by a new technology, as well as for cognitive and psychological reasons.118 The old adage goes: the thing people really hate, more than the way things are, is change. Military innovation poses even more subtle challenges. Adoption of AI may be perceived as especially daunting, because the technology is intangible and difficult to quantify: we can neither touch it nor see it. Additionally, previous lessons of military innovations show the close relationship between platforms and service identity. For example, innovation in military aviation became easier when air branches became independent organizations, separate from armies and navies.119 Similarly, operators of transport or rotary-wing aircraft have often struggled to obtain the necessary recognition and resources from within their respective military services. These dynamics also occur between surface and underwater services, as well as between combat and intelligence or between surveillance and reconnaissance units. It remains to be seen where AI will fit into the culture of military organizations, but algorithms, data and processors are unlikely to be in the ensigns of any military service, at least in the foreseeable future: the tense discussions about counting drone operations as flying hours or assigning medals to drone pilots bear testament to that.120 This is a small, but powerful lesson: in the foreseeable future, some military services could lack interest in, or display insufficient attention to, these domains.121 This is why an AI champion within NATO may be particularly important.122 There is an additional consideration: interoperability would be difficult without coordination among Allies. At the NATO level, a centralized body could play a particularly useful and effective role in this respect. Future discussions could determine whether such a Centre should be independent, like a Centre of Excellence, or sit within the NATO Enterprise structure (natural options being under Allied Command Transformation or in the NATO Communications and Information Agency). There are, however, strong reasons to assign such a Centre a number of specific goals. Lead. The Centre should be at the forefront of NATO’s and the Allies’ AI efforts, including discussions about ethics and ownership of pilot projects (see below) as well as development of targeted solutions to existing problems and challenges. Support. The A3IC should have an interest in helping Allies adopt AI through a set of procedures, roadmaps, best practices and, where possible, readily available solutions, either developed in-house or borrowed from others. From ethics to training, from recruitment to procurement, from cyber security to data management, the Centre could provide important support, especially for some Allies or some of their services that may lack in- house solutions or expertise. Cases in point would be Testing and Evaluation (T&E) and Verification and Validation (V&V): with the adoption of ML, these will have to be rethought, upgraded and updated in order to integrate the non-deterministic nature of algorithms into existing procedures and methods.123 Similarly, in the age of software, procurement needs a major upgrade. In contrast to traditional military platforms, it is faced with a paradigm shift: rather than deliver finished and well-functioning products, it must come up with adaptable solutions that, by their very nature, can never be considered as “done” once and for all.124 Realistically, not all Allies possess the necessary expertise to face such challenges. The Centre could play an important role in these areas. Since the AI ecosystem, as this document shows, is admittedly massive but also scalable, for many Allies it may be much more convenient to rely on common, Alliance-wide capabilities, since they would probably struggle to achieve the required depth and the breadth if left to their own devices. Connect. The Alliance will not be effective if individual Allies’ efforts remain disconnected; and it will be more efficient if Allies are able to build on each other’s progress and achievements. The Centre could play a major role in this respect. For instance, the software community around the world relies on platforms such as GitHub to accelerate software development.125 The Alliance has the opportunity to move in the same direction, enabling Allies to benefit from each other’s progress. Researchers in different fields need the same types of tools, from science workflows to AI-driven experimentation, from testing and evaluation to other domains. If NATO’s A3IC could provide a central repository of AI software, it would connect all the actors, accelerate their work and also address potential failures.126 Similar considerations apply to data. “Usually, the biggest challenges [are] related to getting sufficient high-quality training data”. In fact, “system performance is directly tied to data quantity, quality, and representativeness”.127 For the A3IC, a key goal would be to make training data available, as this would dramatically accelerate Allies’ progress. Recent progress in AI has been possible, because nowadays there are “many open source code libraries and developer tools that allow organizations to use and build upon the work of external communities. As a result, no team or organization has to start from scratch, and may parts that used to require highly specialized expertise have been largely automated”.128 The A3IC could play a similar role in making all tools and tests available. This is particularly important for T&E/V&V activities, as will be discussed later.

### AT: Leaks/Theft

#### **Removing data sharing barriers and establishing agreements on AI development is key towards interoperability**

Greenberg ‘20(Erik Lin-Greenberg, “Allies and artificial intelligence: Obstacles to operations and decision making”, Texas National Security Review, 3(2), 56–76, March 05 2020, https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/)-amc

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](https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/" \l "_ftn108) 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](https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/" \l "_ftn109) 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](https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/" \l "_ftn110) 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.

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](https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/" \l "_ftn117) 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](https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/" \l "_ftn118) These standards ensure “doctrine, tactics, and techniques are developed in harmony” to help allies “operate effectively together while optimizing the use of resources.”[119](https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/" \l "_ftn119)

### AT: Brittle Turn

#### Defense integration and innovation happen quick – even small countries can specialize in specific AI systems.

Husain et al. 18 (Amir Husain, August Cole, and Wendy R Anderson. CEO of Spark Cognition & Board of Advisors for UT Austin’s Department of Computer Science & Member of Council on Foreign Affairs, Senior fellow of Scowcroft Center on Strategy and Security at the Atlantic Council & Fellow of Brute Krulak Center for Innovation and Creativity at Marine Corps University. " As Budget Polemic Drives Headlines, Do Not Lose Track of NATO’s Approach to AI". 07-27-2018. Royal United Services Institute. https://www.europarl.europa.eu/cmsdata/155282/WendyRAnderson\_RUSIArticle.pdf. 6-22-2022.)-cg

Unlike defence industrial bases, which are needed for fighters or tanks, critical AI innovations could come from NATO’s smallest nations, with an Alliance-standard approach ensuring that small states are not crowded out. A set of common NATO AI capabilities matched to the Alliance’s operating concepts can bridge the technical gaps that could leave out states lacking the relevant technology–industry expertise or the ability to implement AI systems in their defence ministries. Moreover, given the complexity of missions around the world, NATO needs to be fully integrated at a mission-systems level, rather than individual states operating individually with incompatible technologies. Technological developments concerning AI are presently advancing with such speed that the trailing behind of any one country with adoption or implementation could undercut whole-of-NATO efectiveness when it is needed most during a crisis. Artificial Intelligence (AI) is becoming a decisive force in the international security environment, with the potential to transform everything from information operations to intelligence analysis to mission planning. Whether NATO takes a unified approach to AI or not is a crucial question for the Alliance to consider. This applies to more than just technology: there is also growing collective responsibility around data, privacy and the power of the state. A NATO AI operational framework can ensure world-leading standards are upheld across the Alliance. Indeed, NATO is working on AI commonality, but it is focused on the question of how much freedom to give autonomous machines. ‘Creating a common standard for describing the role of the human operator and the role of the machine in systems that use AI will help commanders incorporate such systems in their planning processes’, NATO officials wrote in setting-up a study due in 2020 on Human in the Loop Considerations for Artificial Intelligence. ‘In a coalition environment, such systems potentially deploy in parallel during an operation, which requires that NATO commanders understand the subsequent effect on planning and C2’. That is indeed critical, but equally important is considering this at a much higher level. With a new NATO AI standard, NATO can employ AI in a manner that does more good than harm, operationally and bureaucratically speaking. The NATO AI Standard When NATO developed Cold War-era standards on everything from ammunition to aircraft grease-ports, commonality of military hardware was essential in ensuring the feasible collective defense of Europe.

### AT: Unilateral CP

#### CP rips NATO apart and fuels US unilateralism which dooms European relations.

Soare 20 [Simona R. Soare, Simona R. Soare 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., “DIGITAL DIVIDE? Transatlantic defence cooperation on Artificial Intelligence”, European Union Institute for Security Studies, Brief 3, March 2020, [https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%203%20AI\_0.pdf]-amc](https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%203%20AI_0.pdf%5d-amc)

Relatedly, NATO will be increasingly challenged to maintain interoperability and ensure politically relevant contributions, particularly from smaller allies without advanced AI-enabled capabilities. This is because the transatlantic allies operate a mix of new and legacy systems that are diverse and produce data that is fragmented and heterogeneous. Indeed, a replay of the experience in cyber capabilities is entirely possible in AI: a small number of transatlantic partners deploy advanced AI-enabled systems to maintain their full-spectrum military capabilities and the rest either eventually adopt a variety of less sophisticated AI capabilities to remain relatively interoperable or develop AI niche capabilities to enhance their added value to the alliance. This would increase the intra-alliance AI dependence on nations with full-spectrum AI-enabled capabilities, including in the areas of collective decision-making, operations, collaborative capability development and counter-AI. This asymmetry is particularly worrisome for rapid decision-making in NATO, one of the pillars of the Alliance’s adaptation efforts. Wider information asymmetry between transatlantic partners underpinned by asymmetry in AI-enabled capabilities could hinder rapid decision-making between the allies.28 Such dynamics fuel American unilateralism and exacerbate long-standing tensions between the transatlantic partners, as recently demonstrated by the American withdrawal from Syria and the killing of Iranian general Qassem Soleimani. Consequently, European partners will face important ethical, legal and strategic considerations about US operational use of AI-enabled capabilities in Europe and will have to manage the increased risks of European entanglement in an unintended US conflict. This will be a far cry from Europe’s attempt to take back control of its own defence. For these and other reasons, it is difficult to overestimate the importance of active European participation in the formulation of rules for the operational use of AI.

### AT: EU CP

#### Europe start-ups are lagging behind in the tech race due to poor salaries, stock options, and superhubs

Baroudy et. al ‘20 ([Kim Baroudy](https://www.mckinsey.com/our-people/kim-baroudy), head of McKinsey’s Technology, Media & Telecommunications Practice in Europe, Jonatan Janmark, associate partner in the Stockholm office, Tobias Strålin is a partner at McKinsey & Company, Abhi Satyavarapu and Zeno Ziemke, consultants in the San Francisco office, “Europe’s start-up ecosystem: Heating up, but still facing challenges,” McKinsey & Company, October 11 2020, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/europes-start-up-ecosystem-heating-up-but-still-facing-challenges)-amc

Attracting the best talent can be difficult. While Europe has a tech talent cost advantage compared to the United States—salaries for software developers are as much as 50 percent lower in Europe than those in the San Francisco Bay Area or New York City8 —the continent’s start-ups often lack the tools to attract the best talent. Most notably, in many European countries unfavorable equity and stock-option rules make start-ups less appealing to potential employees. For example, more than 75 percent of the EU countries’ stock-option rules analyzed by the European VC firm Index Ventures lagged behind those of the United States.9 At the same time, the significantly lower number of leading tech companies and successful hypergrowth start-ups in Europe reduces the pool of experienced executives and other talent that have hands-on background in building IPO-sized companies. The type of operational knowledge that comes from deep experience launching and exiting from successful start-ups is key to scaling companies through the late stages. Innovation ‘superhubs’ are not as densely packed with resources as those in the United States. “Superhubs” such as Silicon Valley and New York City, which have a high concentration of entrepreneurs, tech talent, and investors, have played a very important role in the success of the US start-up ecosystem. Although London, Paris, Berlin, and Stockholm can be considered the leading hubs in Europe, they have not achieved the same concentration in terms of capital, knowledge, and talent. As a result, only about 30 percent of European start-ups have located their headquarters in a tech superhub—where they might have an easier time attracting talent and funding—versus almost half of US start-ups (Exhibit 8). Furthermore, surveys show that more than 60 percent of founders start their companies where they live or where they have family and support systems.10 Of course, relocating within the United States is not the same as relocating within Europe, given that in the United States the language and culture will generally be the same. However, if COVID-19 means that working remotely or from home becomes more common, this disparity might become less problematic and potentially could lessen the importance of superhubs.

## Add-Ons

### 2AC – Miscalc Addon

#### Uncertainty regarding rules of AI as well as future development makes it vital to capitalize on emerging technologies to minimize escalation, otherwise risking unmanned catastrophe through NC3 automation (this one is prob more for goldilocks affs than regs)

Horowitz and Scharre 19 (Michael C. Horowitz is Director of Perry World House and Richard Perry Professor at the University of Pennsylvania. He is currently on a leave of absence from the University to serve as Director of the Office of Emerging Capabilities Policy at the U.S. Department of Defense. Paul Scharre is the Vice President and Director of Studies at CNAS. He led the Department of Defense (DoD) working group that drafted DoD Directive 3000.09, establishing the department’s policies on autonomy in weapon systems) December 2019 “A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence” [https://arxiv.org/ftp/arxiv/papers/1912/1912.05291.pdf) //](https://arxiv.org/ftp/arxiv/papers/1912/1912.05291.pdf)%20//) ZX

Nuclear weapons are arguably the single most significant weapon system invented in modern history, meaning uncertainty about the viability of nuclear deterrence in the 21st century constitutes one of the most important security risks facing the world.2 This uncertainty is both a product and source of increased tensions in nuclear dyads worldwide. The proliferation of conventional military technologies, such as hypersonic weapons, could further undermine deterrence by potentially undermining traditional modes of escalation management, and as a consequence, nuclear stability. 3 The impact of autonomous systems and artificial intelligence (AI) for nuclear stability remains understudied, however.4 In early 2017, Klaus Schwab of the World Economic Forum argued that the world is on the cusp of a Fourth Industrial Revolution, wherein several technologies – but most prominently AI – could reshape global affairs.5 Many defense experts around the world share Schwab’s recognition of the potentially transformative effects of AI.6 The most prominent statements about the impact of AI on warfare, however, tend to be extreme. Elon Musk, for instance, has vocally contended that AI run amok could risk World War III.7 This overheated rhetoric masks the way that advances in automation, autonomous systems, and AI may actually influence warfare, especially in the vital areas of nuclear deterrence and warfighting. The intersection of nuclear stability and artificial intelligence thus raises critical issues for the study of international politics. Relative peace between nuclear-armed states in the 20th century arguably relied in part on mutually assured destruction (MAD). 8 MAD prevails when each side recognizes that both it and its opponent have an assured nuclear second-strike capability, or that either side can impose unacceptable damage on the other in retaliation against a nuclear attack.9 Threat of mutual destruction ultimately led both the United States and the Soviet Union to deprioritize the role of preemption in their nuclear war plans.10 Furthermore, as Albert Wohlstetter found, the threat of mutual destruction “offer[ed] every inducement to both powers to reduce the chance of accidental war.”11 While there are no known instances of accidental war, there are historical examples of unintended escalation, either in preconflict crises or once a conflict is underway.12 Accidental escalation is when a state unintentionally commits an escalatory act (i.e. due to technical malfunction, human error, or incomplete control over military forces). 13 Inadvertent escalation can also occur, whereby a state unknowingly commits an escalatory act (i.e., an intentional act that unknowingly crossing an adversary’s red line). 14 Accidents have increased tensions between countries on numerous occasions, but have not led to escalation.15 Nuclear-armed states have expended vast resources to minimize the risk of unintentional escalation, knowing that it could lead to catastrophe should it occur. Automation may complicate the risks of escalation, deliberate or unintended, in a number of ways. Automation has improved safety and reliability in other settings, from nuclear power plants to commercial airliners. Used properly, many applications of automation in nuclear operations could increase reliability, reduce the risk of accidents, and buy more time for decision-makers in a crisis. Automation can help ensure that information is quickly processed, national leaders’ desires are swiftly and efficiently conveyed, and launch orders are faithfully executed. On the other hand, poor applications of automation could render nuclear early warning or command-and-control (C2) systems more opaque to users, leading to human-machine interaction failures. Human users could fall victim to automation bias, for example, surrendering their judgment to the system in a crisis Automation is often brittle and lacks the flexibility humans have to react to events in their broader context. The states most likely to be willing to tolerate these risks for the perceived capability gains would be those that have significant concerns about the viability of their second-strike deterrents. Thus, the more a country fears that, in a world without using autonomous systems, its ability to retaliate to a nuclear strike would be at risk, the more attractive autonomous systems may appear. Uninhabited nuclear delivery platforms could undermine nuclear surety, as they could be hacked or slip out of control, potentially leading to accidental or inadvertent escalation. Automated systems could end up reducing decision-maker flexibility by narrowing options, hampering attempts to manage escalation. These dynamics suggest that autonomous systems could influence the potential for nuclear escalation in three ways. First, while many aspects of the nuclear enterprise are already automated in many countries, from early warning and command and control to missile targeting, as autonomous systems improve, states may elect to automate new portions of the early warning and C2 processes to improve both performance and security. From a security standpoint, for instance, increased automation in nuclear early warning may allow operators to identify threats more rapidly in a complex environment. Likewise, automation may help to ensure the dissemination of launch orders in a timely manner in a degraded communications environment. States may also automate – or threaten to automate – nuclear launch procedures in the belief that doing so would provide them with a coercive advantage over adversaries. Second, as military robotics advance, nuclear powers could deploy uninhabited nuclear delivery platforms for a variety of reasons. For instance, a state might deploy nuclear-armed long endurance uninhabited aerial vehicles (UAVs) in the belief that doing so would provide additional nuclear signaling or strike options. They might also look to uninhabited nuclear delivery platforms to bolster their secure second-strike capabilities. Nuclear delivery vehicles – such as torpedoes – capable of autonomously countering enemy defenses or selecting targets might be seen to do likewise. Alternatively, a government might choose to automate its nuclear forces so that a small number of trusted agents can maintain control. This might could be especially attractive for a nuclear-armed regime that fears a coup or other forms of interference by its nation’s military elite. Third, the increased automation of conventional military systems might influence nuclear stability in direct and indirect ways.16 It may enable – or more likely yet, be seen to enable – improved counterforce operations by technologically-advanced states. The ineffectiveness of counterforce operations – and hence the survivability of second-strike deterrents – presently hinges in large part on the difficulty of finding and tracking adversary nuclear launch platforms (mobile missiles or submarines) long enough for ordnance to be delivered. Machine learning algorithms and other applications of artificial intelligence could, in principle, improve states’ abilities to collect and sift through large amounts of data in order to locate and track such targets, though it is important to recognize limitations to any developments given the real-time requirements for a disarming strike. Likewise, military autonomy could enable the deployment of conventional autonomous systems designed to shadow and/or attack nuclear-armed submarines. Furthermore, if automation gives (or is perceived to give) one side in a competitive dyad a significant conventional military advantage, the weaker side may feel compelled to rely more heavily on nuclear weapons for deterrence and warfighting. These issues surrounding the potential impacts of artificial intelligence are magnified by uncertainty about the trajectory of technological developments. This article first proceeds by clarifying what autonomous systems are and clarifying often-tricky definitional issues surrounding artificial intelligence. It then lays out some key theoretical expectations. Second, the article explores the impact of autonomous systems on early warning and nuclear command and control, as well as intelligence, surveillance, and reconnaissance (ISR) relevant for nuclear systems, in the context of recent research. Third, the article discusses the potential for uninhabited nuclear delivery platforms and vehicles featuring new kinds of automation. Fourth, the article describes the way conventional autonomous systems could both directly and indirectly influence nuclear stability. Finally, the article concludes by assessing the net likely impact of autonomous systems on nuclear stability and describing potential pathways for future research. The analysis argues that the impact of autonomous systems could depend on the specific application – both where automation falls in the nuclear enterprise but also how it is implemented in terms of design, human-machine interfaces, training, and operator culture.

### 2AC- Cyber Addon

#### Coordinated AI ensures effective intelligence, surveillance, and reconnaissance – that stops cyber-attacks and escalation.

Hill ‘20 [Steven Hill, served until February 2020 as Legal Adviser and Director of the Office of Legal Affairs (OLA) at the NATO International Staff, "AI's Impact on Multilateral Military Cooperation: Experience from NATO," 4-27-2020, American Journal of International Law | Cambridge Core, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ais-impact-on-multilateral-military-cooperation-experience-from-nato/3AEF22AA22550A10B75DD74A806D4D18]/lf

AI Applications from a NATO Perspective It is useful to complement this description of NATO’s fairly nascent policy work on military applications of AI with a brief overview of the types of applications that one hears most discussed in NATO circles. Given the amount of academic, media, and political attention to the issue of lethal autonomous weapons systems (LAWS), it might come as a surprise that it is the far less high-profile or headline-grabbing applications of AI that receive attention within NATO. This may well be because LAWS are already being discussed by a Group of Governmental Experts within the Geneva-based framework of the Convention on Certain Conventional Weapons, thus making Allies hesitant to duplicate discussions in Brussels. However, the reason that the issue of LAWS—however important the debates involved—is not on the forefront of the agenda at NATO is likely more straightforward: that current and foreseeable technology suggests different, perhaps more prosaic applications, for AI in the military sphere. This essay focuses on two: (1) intelligence, surveillance, and reconnaissance (ISR); and (2) cyber defense. The development and use of AI-enabled applications in each of these areas clearly presents both opportunities and challenges. Enhancing the information available to support decision-making is one of NATO’s priorities. ISR is based on information-gathering from a variety of assets deployed across domains. The information or data gathered from both NATO and national assets can then be fused together to help identify patterns and trends in support of situational awareness and operational decision-making. Since this data will likely be too voluminous for traditional human analysis, NATO can leverage AI-enabled systems to comb through these datasets. In this way, NATO can apply AI to enhance situational awareness and improve decision-making, a potentially considerable advantage given the challenges of getting all Allies up to speed on rapidly evolving situations. AI applications can also be used in the context of cyber defense, where NATO has a defensive mandate focused on defending NATO’s networks and supporting Allies as they defend their own networks. AI-based applications cover areas such as preemptive patching and the taking of corrective action on the basis of a constant analysis of low-level and recurrent patterns of attacks and cyber threats across networks, all done more quickly and with greater precision. Moreover, the more information exchanged on the nature of attacks in a variety of networks, the easier it is to identify trends in multinational cyber threats. While the use of AI in both these contexts could potentially increase the speed and quality of multinational military cooperation, it clearly also can pose difficulties. For example, increasing speed could be perceived as fueling pressure for inappropriately accelerated action. This kind of acceleration of usual processes might be perceived as going against “normal” NATO decision-making in a number of ways: it might be seen as evading the political control exercised by the North Atlantic Council, overriding the consensus decision-making that applied within the Alliance, being susceptible to misinterpretation or being seen as escalatory in nature, or otherwise leading to unpredictable results. In an extreme case, Allies might see these situations as inconsistent with NATO’s collective defense mandate. This might result in a backlash against the use of AI-enabled military applications, precisely at a time when the Alliance needs to maintain an edge with them. In other words, as with many issues involved in multinational military cooperation, the problem may ultimately boil down to one of trust.

### 2AC – Racism Addon

#### Racism in AI is present and developing. Further implementation exacerbates structural racism and eliminates colored bodies. (really good structural impact card for soft left version, but might need to run with “AI norms spills over” type cards to be completely effective)

**Asaro 19** (Peter M. Asaro (M’10) Dr. Asaro received his PhD in the history, philosophy and sociology of science from the University of Illinois at UrbanaChampaign, Urbana, Illinois, USA, where he also earned a Master of Computer Science degree. October 17, 2019 Racism and Fully Autonomous Weapons [https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/Call/campaigntostopkillerrobots.pdf //](https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/Call/campaigntostopkillerrobots.pdf%20//) ZX

The rise of artificial intelligence is largely due to an increase in power, memory and speed of computers, and the availability of large quantities of data about many aspects of our lives. Through the commercial application of big-data, we are increasingly being sorted into different classifications and stereotypes. In its most benign form, this stereotyping is being used to sell us products via targeted advertising, however, in its most egregious application, we see the weaponization of new information technologies utilize similar classifications based on biased algorithms, to which the consequences for certain communities could be deadly. In this paper I focus on fully autonomous weapons that are currently being developed for military and law enforcement purposes; and their potential threat to the human rights of marginalized communities, in particular persons of color intersectionally. This paper will also consider the systemic nature of racism and how racism would be reinforced and perpetuated by fully autonomous weapons. Fully autonomous weapons can select and attack targets without meaningful human control, they operate based on algorithms and data analysis programming. In essence, this means that machines would have the power to make life-and-death decisions over human beings. The trend towards more autonomy in weaponry without adequate human oversight is alarming especially when we know that digital technologies are not racially neutral. Moreover, when it comes to artificial intelligence (AI) there is an increasing body of evidence that shows that racism operates at every level of the design process and continues to emerge in the production, implementation, distribution and regulation. In this regard AI not only embodies the values and beliefs of the society or individuals that produce them but acts to amplify these biases and the power disparities.iii One example of racism manifesting in AI is the under-representation problem in science, technology, engineering and mathematics (STEM) fields, which in itself is a manifestation of structural racism and patriarchy in western society. Technologies in the west are mostly developed by white males, and thus perform better for this group. A 2010 study by researchers at the National Institute of Standards and Technology (NIST) and the University of Texas, found that algorithms designed and tested in East Asia are better at recognizing East Asians, while those designed in Western countries are more accurate at detecting Caucasians. Similarly, sound detecting devices perform better at detecting male, Anglo-American voices and accents, as opposed to female voices, and non-Anglo-American accents. Research by Joy Buolamwini,v reveals that race, skin tone and gender are significant when it comes to facial recognition. Buolamwini demonstrates that facial recognition software recognizes male faces far more accurately than female faces, especially when these faces are white. For darker-skinned people however the error rates were over 19%, and unsurprisingly the systems performed especially badly when presented with the intersection between race and gender, evidenced by a 34.4% error margin when recognizing dark-skinned women. Despite the concerning error rates in these systems, commercially we already see adaptations of faulty facial recognition systems being rolled out in a variety of ways from soap dispensers to self-driving cars. The issue here is what happens if law enforcement and national security become reliant on a system that can recognize white males with just 1% error rate yet fails to recognize dark-skinned women more than one-third of the time? These types of applications of new information technology fail people of color intersectionally at a disturbing rate. The fact that these systems are commercially available reveals a blatant disregard for people of color, it also positions "whiteness" as the norm, the standard for objectivity and reason. These applications of new information technology including their weaponization favors whiteness at the expense of all others, it is not merely a disempowerment but an empowerment. In real terms, racism bolsters white people's life chances. As we all grew up in a white-dominated world it is not surprising that the vast majority of white people operate within, benefit from and reproduce a system that they barely notice. This is a long-held reality and it is a fundamental problem that we now see infiltrate technology. Historical or latent bias in data is another issue, this is created by frequency of occurrence, for example in 2016 an MBA student named Rosaliaviii discovered that googling "unprofessional hairstyles for work" yielded images of mainly black women with afro-Caribbean hair, conversely when she searched "professional hair" images of mostly coiffed white women emerged, similar google search results are still seen today. This is due to machine learning – algorithms; it collects the most frequently submitted entries and therefore reflects statistically popular racists sentiments. These learnt biases are further strengthened, thus racism continues to be reinforced. A more perilous example of this is in data-driven, predictive policing that uses crime statistics to identify "high crime" areas and then subjects these areas to higher and often more aggressive levels of policing. Crime happens everywhere, however when an area is over-policed such as communities of color that results in more people of color being arrested and flagged as "persons of interest" thus the cycle continues. In 2017, Amnesty International launched a report called "trapped in the Matrix",ix the report highlighted racially discriminatory practices by the UK police force and their use of a databasecalled the "Gangs Matrix" which inputs data on "suspected" gang members in London. As of October 2017, there were 3,806 people on the Matrix, 87% of those are from black, Asian and minority ethnic backgrounds and 78% are black, a disproportionate number given that the police's own figures show that only 27% of those responsible for serious youth violence are black. Amnesty stated that some police officers in the UK have been acting like they are in the "Wild West", making false assumptions about people based on their race, gender, age and socioeconomic status. As a result, individuals on the Matrix database are subject to chronic overpolicing. With black people six times more likely to be stopped and searched than white people, and ten times more likely to be convicted of drug-related offenses. This system not only interferes with their right to privacy, Amnesty claims that the police often share the Matrix with other local agencies such as job centers, housing associations, social services, schools and colleges. In several cases, this has led to devastating impacts on people's social and economic lives because they are listed as "nominal" gang members, a label which is deliberately vague and stigmatizing. The nature of systemic racism means that it is embedded in all areas of society, the effects of this type of oppression doesn't easily dissipate. Through the continual criminalization and stigmatization of people of color, systemic racism operates by creating winners and losers regardless of what people actually do. This is also the way that it redistributes opportunities and resources based on nothing other than privilege. Given that the UK, as well as five other countries are developing fully autonomous weapons to target, injure and kill based on data-inputs and pre-programmed algorithms, we can see how long-standing inherent biases, pose an ethical and human rights threat. Where some groups of people will be vastly more vulnerable than others, fully autonomous weapons would not only act to further entrench already existing inequalities but could exacerbate them and lead to deadly consequences. Legalities As AI technology advances, the question of who will be held accountable for human rights abuses is becoming increasingly urgent. Machine learning and AI, effect a range of human rights including privacy, freedom of expression, freedom of assembly, the right to non-discrimination and equality, the right to life and the right to human dignity. Holding those responsible for the unlawful killings of people of color by law enforcement and the military is already a huge challenge in many countries, however, this issue would be further impaired if the unlawful killing was committed by a fully autonomous weapon. Who would be held responsible: the programmer, manufacturer, commanding officer, or the machine itself? Lethal force by these weapons would make it even easier for people of color to be at the mercy of unlawful killings and far more difficult to obtain justice for victims of color and their families. According to Reni Eddo-Lodge racism perpetuates partly through malice, carelessness and ignorance, it acts to quietly assist some, while hindering others.xi It is within this framework that we must grapple with race and the weaponization of new information technologies. In this regard, we should ask ourselves who controls these technologies and what do they think they know about the people they are "classifying"? What are the politics of these relationships and the deeply-rooted systemic forms of discrimination? Who benefits from these technologies and how? There is a long history of people of color being experimented on for the sake of scientific advances from which they have suffered greatly but do not benefit. An example of this is from James Marion Sims, known as the father of gynecology for reducing maternal death rates in the US, in the 19th century. He conducted his research by performing painful and grotesque experiments on enslaved black women. "All of the early important reproductive health advances were devised by perfecting experiments on black women,".xii Today, the maternal death rate for black women in the US is three times higher than it is for white women. Thus, when it comes to new information technology, facial recognition systems, algorithms and automated and interactive machine decision-making, communities of color are often both deprived of their benefits and subjected to their consequences. This paradox where science is inflicted on communities of color rather than aided by it must be addressed. We must be vigilant against deeply rooted social problems taking root in the technical infrastructure that we create. We must work towards a zero policy on racism in technology, and not weaponize racism in technology. If racism and killer robots are allowed to co-exists these weapons will be used discriminately against people of color and other marginalized groups. For these and many other ethical, moral, human rights, legal and humanitarian reasons the Campaign to Stop Killer Robots, numerous governments, regional groups, tech workers, experts, scholars and the UN Secretary-General are all calling for a legally binding instrument to prohibit fully autonomous weapons xiii We call on the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance to condemn fully autonomous weapons and the human rights threat they pose to people of color; and to support a prohibition treaty that will preserve meaningful human control over the use of force and prohibit fully autonomous weapons.