# Neg – AI Logistics Updates – FMPS

## Non-Democratic Country PIC

### 1nc

#### TEXT: The United States federal government should substantially increase its artificial intelligence military logistics with Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Norway, Romania, Slovakia, Slovenia, Spain, and the United Kingdom

#### Expansion of non-democratic governments of NATO states diminishes alliance credibility and risks a slide to global authoritarianism

Jonathan **Katz and** Torrey **Taussig 18**, "An inconvenient truth: Addressing democratic backsliding within NATO," Brookings Jonathan Katz is director of Democracy Initiatives and a senior fellow with The German Marshall Fund of the United States (GMF) based in the Washington, DC, office. Torrey Taussig was the research director for the Project on Europe and the Transatlantic Relationship at Harvard Kennedy School's Belfer Center. 7-10-2018, https://www.brookings.edu/blog/order-from-chaos/2018/07/10/an-inconvenient-truth-addressing-democratic-backsliding-within-nato/, accessed 6-21-2022//cpd

There is also significant democratic backsliding among NATO member states. The cast of illiberal characters—who are leading the charge in the wrong direction—includes the recently reelected and empowered Turkish President Recep Tayyip Erdoğan and his Justice and Development Party (AKP), Jaroslaw Kaczynski’s Law and Justice (PiS) Party in Poland, and Hungarian Prime Minister Viktor Orbán and the ruling Fidesz Party. Each has proven more than willing to repress free media, dismantle checks and balances, demonize political opposition, clamp down on civil society, and diminish the rule of law. America’s democratic system and norms under President Trump are also under duress; as a result, Freedom House downgraded the country’s score on the basis of weakening political rights and civil liberties.

Despite these alarming developments, NATO leaders have relegated democratic backsliding to the backburner. Opponents of making the case for democracy within NATO might argue that pushing Ankara, Warsaw, and Budapest too hard on their commitments to good governance will exacerbate already tense divisions in the alliance. Others might say that Russia would be the prime beneficiary of a contentious democracy discussion at NATO. Yet this is a counterproductive approach with current and potential costs to NATO’s future. Here are three security-based reasons why the United States and NATO should care about democratic backsliding, and actions the alliance can take to address them.

1Russia is already benefiting from and effectively leveraging its relationships with Hungary and Turkey to exacerbate discord within Europe and NATO. Viktor Orbán and Vladimir Putin see one another as allies in their disdain for the European Union and Orbán has courted Russian financial and political support as he builds an illiberal democracy in Hungary. Russian propaganda also finds fertile ground in Hungarian media. A 2018 Senate Foreign Relations Committee report noted that Russian state-owned media content “by Sputnik and RT is widely referenced by pro-government news sources in Hungary.” The report cited Orbán as the EU and NATO’s most supportive leader of Putin’s worldview and leadership. Acting as the Russian “camel’s nose under the tent,” Orbán is thwarting Ukraine and NATO’s partnership efforts by blocking the Ukraine-NATO Commission from meeting at the upcoming summit.

In Turkey, Erdoğan has rattled the NATO alliance by pursuing a deal to purchase the S-400 missile system from Russia. In addition to hurting NATO’s ability to cooperate on security, the system is also not compatible with NATO’s defenses. Through arms and energy deals, Putin uses Turkey as a wedge to divide NATO. Similarly, Erdoğan might see his deals with Putin as a way to free Turkey from Western leverage, particularly as European states push back on his brand of authoritarian politics by cutting EU pre-accession funds. After winning the recent twin parliamentary and presidential elections, an emboldened Erdoğan will likely become an even more problematic partner for NATO.

President Putin is building ties with illiberal leaders across Europe while attacking fundamental elements of Western democracies.

Other illiberal and populist governments, including Italy’s new anti-establishment government, could follow suit in enhancing their partnerships with Russia, creating future intelligence-sharing and cohesion problems for the alliance. President Putin is building ties with illiberal leaders across Europe while attacking fundamental elements of Western democracies, including electoral process and open information spaces.

2There is a strong link between democratic governance and security gains. Liberal democracies have historically been less likely to experience intra- and interstate conflict, generate refugees, and harbor violent extremists. They are also better at maintaining transparent institutions, civilian control of the military and intelligence services, and working together on confidence-building measures, all of which are core features of NATO’s ability to collectively defend its members. On the other hand, corruption and insecurity grow under politicized institutions and poor rule of law. This hurts NATO’s renewed efforts to combat terrorism, as military and security communities have long acknowledged the connection between corruption and the existence of criminal networks, traffickers, and terrorists within state borders.

Corruption also opens space for Russian kleptocratic networks close to Putin to operate and gain influence. For example, in 2014 Orbán awarded Rosatom, a Russian state-owned nuclear company, the sole contract to build two nuclear plants in Hungary in exchange for a 10 billion euro loan from Moscow. The Hungarian parliament, dominated by Orbán’s Fidesz Party, then passed a rushed vote to keep data from the nuclear deal confidential for 30 years in the name of “national security.” The deal diminished transparent economic competition within the European Union and solidified Hungary and Russia’s energy ties.

3Distrust among allies hurts alliance interoperability. The PiS Party’s assault on independent media and the Constitutional Court, including efforts last week to summarily force out 27 Polish Supreme Court justices, have isolated Poland from France and Germany, diminishing trust among the European nations. This could make it increasingly difficult for Washington to gain consensus on joint decisions, communications, and operations. If NATO is dedicated to building resiliency along Russia’s periphery by placing multi-national battalions in Poland, then it should not ignore the accountable institutions that would strengthen this joint effort.

#### A slide to worldwide Digital Authoritarianism is worse than extinction!

Di **Minardi 20** “The grim fate that could be ‘worse than extinction’,” BBC Future, 15th October 2020 https://www.bbc.com/future/article/20201014-totalitarian-world-in-chains-artificial-intelligence//cpd

Though global totalitarianism is still a niche topic of study, researchers in the field of existential risk are increasingly turning their attention to its most likely cause: artificial intelligence.

In his “singleton hypothesis”, Nick Bostrom, director at Oxford’s FHI, has explained how a global government could form with AI or other powerful technologies – and why it might be impossible to overthrow. He writes that a world with “a single decision-making agency at the highest level” could occur if that agency “obtains a decisive lead through a technological breakthrough in artificial intelligence or molecular nanotechnology”. Once in charge, it would control advances in technology that prevent internal challenges, like surveillance or autonomous weapons, and, with this monopoly, remain perpetually stable.

If the singleton is totalitarian, life would be bleak. Even in the countries with the strictest regimes, news leaks in and out from other countries and people can escape. A global totalitarian rule would eliminate even these small seeds of hope. To be worse than extinction, “that would mean we feel absolutely no freedom, no privacy, no hope of escaping, no agency to control our lives at all", says Tucker Davey, a writer at the Future of Life Institute in Massachusetts, which focuses on existential risk research.

“In totalitarian regimes of the past, [there was] so much paranoia and psychological suffering because you just have no idea if you're going to get killed for saying the wrong thing,” he continues. “And now imagine that there's not even a question, every single thing you say is being reported and being analysed.”

“We may not yet have the technologies to do this,” Ord said in a recent interview, “but it looks like the kinds of technologies we’re developing make that easier and easier. And it seems plausible that this may become possible at some time in the next 100 years.”

AI and authoritarianism

Though life under a global totalitarian government is still an unlikely and far-future scenario, AI is already enabling authoritarianism in some countries and strengthening infrastructure that could be seized by an opportunistic despot in others.

“We've seen sort of a reckoning with the shift from very utopian visions of what technology might bring to much more sobering realities that are, in some respects, already quite dystopian,” says Elsa Kania, an adjunct senior fellow at the Center for New American Security, a bipartisan non-profit that develops national security and defence policies.

In the past, surveillance required hundreds of thousands of people – one in every 100 citizens in East Germany was an informant – but now it can be done by technology. In the United States, the National Security Agency (NSA) collected hundreds of millions of American call and text records before they stopped domestic surveillance in 2019, and there are an estimated four to six million CCTV cameras across the United Kingdom. Eighteen of the 20 most surveilled cities in the world are in China, but London is the third. The difference between them lies less in the tech that the countries employ and more in how they use it.

What if the definition of what is illegal in the US and the UK expanded to include criticising the government or practising certain religions? The infrastructure is already in place to enforce it, and AI – which the NSA has already begun experimenting with – would enable agencies to search through our data faster than ever before.

In addition to enhancing surveillance, AI also underpins the growth of online misinformation, which is another tool of the authoritarian. AI-powered deep fakes, which can spread fabricated political messages, and algorithmic micro-targeting on social media are making propaganda more persuasive. This undermines our epistemic security – the ability to determine what is true and act on it – that democracies depend on.

### 2nc – turkey ai bad

#### Turkey expanding digital authoritarianism into AI greenlights further human rights abuses and anti-democratic control

Fatma **Timucin 21,** “8-BIT IRON FIST: DIGITAL AUTHORITARIANISM IN COMPETITIVE AUTHORITARIAN REGIMES: THE CASES OF TURKEY AND HUNGARY”, 8 July 21, https://research.sabanciuniv.edu/id/eprint/42417/1/10337574.pdf//cpd

Unfortunately, in the last decade, Turkey has garnered international attention with its violation of free media. As stated in the literature (Yıldırım, Baruh, and Çarkoğlu 2020), her track record in media freedom has been far from perfect since the 1990s. Governments have displayed consistent patterns of restriction and punishment for opposition outlets as well as apparent favoritism towards pro-government ones. The remaining content opted for appealing to the relatively stable opposition voter base. The electoral success of Justice and Development Party (Adalet ve Kalkınma Partisi - AKP) back in 2002 failed to signal a deviation from this path in its early years. As 2021 marks their 19th consecutive year in government, we can observe a steady increase in media pressure over AKP’s time at the helm of parliament. The key argument of high political and societal polarization stands (Çarkoğlu, Baruh, and Yıldırım 2014). In addition, another process we must observe is the democratic backsliding Turkey has experienced over the last two decades (Yıldırım, Baruh, and Çarkoğlu 2020). Indubitably, consequences of the accelerating authoritarianism are evident, with Turkey now being dubbed as “the largest prison for journalists” (Eski 2019). Turkey, especially the “New Turkey” Erdoğan declared after the 2011 legislative election victory, paints an illustrative example of media violations. Admittedly, Turkey’s shortcomings in media freedom precede Erdoğan and his party. The media has, notoriously, stayed in line with a multitude of governments and changed its discourse in accordance. Sensitive topics relating to ethnic and religious minorities were unanimously avoided. 1980 coup provided a window of opportunity as the media expressed more diversity thanks to democratic transition (Bayram 2010). Similar to Latin America (Guerrero 2014), a wave of deregulation in the early 1990s resulted in further commercialization (Yıldırım, Baruh, and Çarkoğlu 2020) and led to “captured liberal” media. It is necessary to mention here that the literature on political communication refers to both direct (or classic) and indirect censorship (Shadmehr and Bernhardt 2015) over media in its “captured” aspect. Hence, with 22 the direct and indirect censorship media is now facing, Turkey’s media freedom has hit an unprecedented low. The following chapter aims to describe the process of the Turkish case of digital authoritarianism under AKP’s rule regarding tools and strategies mentioned in the previous section. Three strategies are essential: media ownership and leverage of government founded upon crony relationships, censorship and bans on alternative media, intimidation of its users by abuse of legislative framework, and lastly, employment of manipulation by trolls and bot accounts. 3.1 Media Ownership: Creating a Government-Friendly Media Landscape by Crony Capitalism As is the case with the general populist rhetoric, Erdoğan and AKP came to power as challengers to the existing regime and status quo. As a prominent party figure, Erdoğan has explicitly been vocal about his distaste in media since the beginning, for its being owned by the “elite” and maintaining the status quo. Another factor of utmost importance in shaping this attitude was Erdoğan’s experience in Refah Partisi (Welfare Party). Existing media outlets held Erdoğan and RP in a negative light. This was made evident with the four months imprisonment sentence Erdoğan received due to reciting a poem in 1997. Media coverage regarding the adjudication showed apparent enthusiasm about the unfolding of events, with the most memorable headline being “He will not be able to become even a headman” (Radikal 1998). This headline became a central piece of Erdoğan’s populist rhetoric in underlining “the people’s” triumph over the preceding regime in later years. In combination, the two motives mentioned above propelled AKP and Erdoğan to replace the media with a pro-government one. Control over traditional media has set the stage for AKP’s digital authoritarianism. As the media became tied to conglomerates owning several pro-AKP outlets, said outlets’ news sites became a projection of their traditional counterparts. In tandem with the increasing control, ‘professional’ digital media became dominantly in favor of the government. 23 Figure 3.1 Democracy Index Scores DemocracyIndexOverallScore Turkey’s descend into competitive authoritarianism came gradually. As Figure 11 shows, it is not unique in this aspect that each of the four countries mentioned throughout this thesis has experienced a slight but consistent decrease in their democracy scores over the last fourteen years. AKP’s media control was no different, a ‘patient struggle’ against the conventional media (Aladağ 2013). Between 2014 and 2018, the asymmetry in media ownership in pro-government and opposition was made official. This clear government bias was the consequence of a series of changes that took place since 2002. By buying outlets and shifting ownership to businessmen with close ties to the government, AKP has laid the ground for what came to be called havuz medyası by its opposition.

### 2nc – hungary ai bad

#### Hungary’s digital authoritarianism creates positive feedback loops of democratic backsliding

Fatma **Timucin** 07-08- **21,** “8-BIT IRON FIST: DIGITAL AUTHORITARIANISM IN COMPETITIVE AUTHORITARIAN REGIMES: THE CASES OF TURKEY AND HUNGARY”, 8 July 21, https://research.sabanciuniv.edu/id/eprint/42417/1/10337574.pdf//cpd

The case of Hungary has garnered recent scholarly attention regarding its democratic trajectory in the latest years. As 2021 marks Victor Orbán’s eleventh year holding the position of Prime Minister, Hungary has turned increasingly authoritarian. The country has accomplished an unfortunate first, as it is the only non-democratic member of the EU since 2020 (Repucci 2020). In turn, several NGOs, international organizations, and member countries have issued demands of political sanctions on Hungary in an attempt to reverse the democratic backsliding it is facing. Orbán’s regime can be characterized by populism and national conservatism. As a distinguishing quality, Orbán openly advocates for an ‘illiberal state’ in advancing national conservatism. His shift to right-wing became apparent in his first term in office between 1998-2002. Following two elections favored the Socialist Party, resulting in a drastic change in the government. However, Orbán’s Fidesz managed to keep its popularity in later years, and coupled with the Socialist’s decreasing voter support, won the election by a landslide in 2010. The subsequent decade has solidified Orbán’s grip on power as Fidesz constituted the majority in the parliament after his coalition with Christian Democrats. This allowed Orbán to pass several constitutional and legislative reforms. The consequences of said reforms spell out a perfect example of the “executive aggrandizement” (Bermeo 2016) pointed out in democratic backsliding literature. Simultaneously, Orbán expanded his influence, blurred the boundaries of executive decision-making, and grasped the popular vote. His maintaining of popular support is linked to several causes in the literature, such as the weak democratic tradition as a result of the post-soviet context (Krygier 2019), deepening of social cleavages (Palonen 2009), and rising Euro-scepticism resulting from a clash of values (Furedi 2017). An overlooked factor of Orbán’s success lies in his gradual capture of the media network, resulting in an enormous asymmetry in pro-government and opposition narratives. Although recent scholarly work aimed to fill the gap in the literature (Fabry 2020; Serdült 2020; Zgut et al. 2020), the issue was raised only after Hungary became a competitive authoritarian regime. 41 An extensive recollection of Orbán’s attitude towards media is hard to come by. In contrast, with many of his populist counterparts, Victor Orbán openly targeted free media since he assumed office. Independent media outlets shrank in numbers and the variety of content they can offer over time. In his crusade against opposition voices, Orbán instrumentalized takeovers as well as restriction and persecution of journalists. One of the last remaining independent media outlets, Index.hu, was met with a change of staff on the grounds of political motivation (Index 2020) in Fall 2020. Calls for the EU to intervene and protect freedom of speech through political pressure were made (IPI 2020), although there is no action taken insofar. In building control over the media, the case of Hungary was specifically successful for its implementation of all three strategies at once: legislative action, financial manipulation, and political pressure (Altena 2017); and the organizational grasp of Fidesz and Orbán resulted in perpetual democratic backsliding where linkage and leverage to EU fell short (Sandoval 2018). The following chapter offers a breakdown of the building and practice of Victor Orbán’s strategies of digital authoritarianism. The case of Orbán’s digital authoritarianism is a valuable contribution to literature in showing the solidification of an increasingly aggressive pro-government media landscape. Systematic violation of freedom of speech aids populist leaders like Orbán in spreading and legitimizing their rhetoric as the one and only ‘truth.’ Diminishing opportunities in accessing alternative sources of information further contributes to democratic backsliding and creates a positive feedback loop, which is why it is worthy of scholarly attention with regards to both digital authoritarianism and populism literatures.

### 2nc – democracy backsliding

#### Turkey’s anti-democratic government decks NATO credibility and risks US security

Michael **Poznansky**, 10-13-20**16**, "NATO members are supposed to be democratic. What happens when Turkey isn’t?," Washington Post, https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/13/nato-members-are-supposed-to-be-democratic-what-happens-when-turkey-isnt/, accessed 6-25-2022//cpd

A core principle of the North Atlantic Treaty Organization (NATO) is that member states adhere to democratic values. So what happens now that Turkey, a longtime NATO member, has suspended a number of legal protections in the weeks and months following the July 15 coup attempt?

Immediately after part of the military tried to overthrow his government, Turkish President Recep Tayyip Erdogan retaliated with a widespread purge of large numbers of police officers, judges and soldiers. By late July, the Turkish government’s crackdown had extended to the private financial sector, as well as the country’s universities. The government detained as many as 50,000 in what one news report called “the biggest purge in Turkey’s modern history.”

How Erdogan’s anti-democratic government made Turkey ripe for unrest

Turkey’s ties with the West are strained

As discussed here in the Monkey Cage, Erdogan met with Russian President Vladimir Putin in early August after criticizing the U.S.-European response to the coup. That Erdogan sought closer ties with Putin is a remarkable outcome in light of the fact that Turkey and Russia have been at loggerheads over Syria.

From Turkey’s perspective, NATO and the West may have “failed the solidarity test” by offering Erdogan little reassurance after the coup attempt. Washington, for instance, made no promise to grant Turkey’s extradition request for Fethullah Gulen, the U.S.-based Turkish cleric who Erdogan claims was the coup’s mastermind. AWhile the two nations have been cooperating in the ongoing fight against the Islamic State, significant tensions remain.

Why it’s good for dictators to have dictator friends

These recent developments — and years of creeping authoritarianism by Erdogan and his AKP party — have led some foreign policy analysts to call for Turkey’s expulsion from NATO.

Doug Bandow at the Cato Institute called for a “civil divorce,” noting that “As Ankara moves toward an authoritarian one-party state, its membership in NATO becomes ever more incongruous.”

Another Cato scholar, Ted Galen Carpenter, last year wrote that “NATO is supposed to be an alliance of peaceful democracies. Yet evidence continues to mount that Turkey fails to meet [that] standard.” More recently, Carpenter wrote, “Does America really want to risk its security to protect such allies, especially when it purports to lead an alliance of enlightened democracies?”

#### Hungary, Turkey, and Poland threaten NATO’s core values

Nicholas **Burns 18,** Professor of the Practice of Diplomacy and International Relations at the Harvard Kennedy School, former NATO ambassador. “"NATO at Seventy: An Alliance in Crisis," Belfer Center for Science and International Affairs. 10-19-2018, , https://www.belfercenter.org/publication/nato-seventy-alliance-crisis, accessed 6-21-2022//cpd

Upholding NATO’s Democratic Values

NATO is struggling to confront a potentially cancerous threat from within. Three allied governments—Poland, Hungary and Turkey—have undermined their own democracies in varying degrees by suppressing free speech and a free press and limiting the independence of the courts.13 As NATO is, first and foremost, an alliance of democracies, the actions of these governments threaten the core values—democracy, individual liberty and the rule of law—to which each ally is committed in the North Atlantic Treaty.

Nearly every current and former NATO official with whom we talked for this report worried that a recommendation for NATO to discipline these anti-democratic governments would be highly problematic and divisive. Nonetheless, we believe NATO must find a way to shine a light on these recalcitrant allies. For example, NATO could review annually each ally’s democratic practices, perhaps in a report prepared by a high-level, outside group. Allies that violate basic democratic standards could be suspended from NATO military exercises or denied access to NATO training and common infrastructure funding.

More than one European mentioned to us the ironic fact that the U.S. itself may be chastised for a deterioration of its own democratic standards in such a process. Nevertheless, ignoring this challenge of democratic principles will undermine the core convictions that brought NATO together seventy years ago.

#### The rise in illiberalism within NATO is leading to democratic backsliding

David Deulofeu **AntúNez** **18**, David Deulofeu Antúnez is a first-year M.A. candidate in Security Policy Studies at the Elliott School of International Affairs "NATO’s Trojan Horse: How Democratic Deconsolidation and Populism are Weakening the Alliance — THE INTERNATIONAL AFFAIRS REVIEW," INTERNATIONAL AFFAIRS REVIEW, 11-28-2018 https://www.iar-gwu.org/blog/2018/11/29/natos-trojan-horse-how-democratic-deconsolidation-and-populism-are-weakening-the-alliance, accessed 6-21-2022//cpd

The North Atlantic Treaty Organization (NATO) is facing an internal problem that could permanently weaken the Alliance. In recent years, we have seen the rise of a nationalist-populist wave in Europe and the United States: Viktor Orbán of Hungary, the Kaczynski in Poland, and President Donald Trump in America. This rise in illiberal world leaders has led to significant democratic backsliding in NATO countries, which pose a grave threat to NATO’s strength in the face of an aggressive and revisionist Russia.

How is Democratic Backsliding Affecting the Alliance?

Democratic governance and strong institutions are as much a cornerstone of the Alliance as is collective defense. Article II of the North Atlantic Treaty (also known as the Washington Treaty) stresses the importance of “states’ promises to strengthen free institutions within their borders,” underscoring the vital democratic aspects of the alliance. Within NATO today, however, some states are shifting away from the core tenets of Article II and are actively conspiring to undermine the same institutional channels that brought them to power. These regressions of democracy create vulnerabilities that can be exploited by NATO adversaries, namely the Kremlin.

In Hungary, Orbán’s increasingly authoritarian Fidesz government has taken an increasingly pro-Russia stance, doling out energy contracts to the country’s oligarchs and calling for Hungary to model itself a similarly to Russia’s illiberal state. In Turkey, the rise of Recep Tayyip Erdogan has resulted in members of the military being sacked and indiscriminate jailing of journalists and academics, while leaving no real opposition to his rule. This in turn has led to closer ties between Ankara and Moscow, especially in matters of defense and the ongoing Syrian civil war. Poland continues to see Russia as both an adversary and a threat; however, Poland’s judiciary reform has effectively turned the high court into a PiS puppet while media repression has simultaneously turned Poland into both a victim and purveyor of disinformation campaigns, further isolating it from its allies and European partners. Democratic backsliding and increased illiberal leaders in NATO countries have opened the door for Russia to engage in an influence campaign, and to pull those countries away from the Liberal Western Order the Alliance is founded on.

Democratic backsliding weakens NATO internally by making cohesion, trust, and operations more difficult. Democracies tend to foster cooperation and trust; autocracies are always looking to blame “the other.” Within NATO, we are seeing bigger wedges being driven into member states, as illiberal regimes criticize their democratic allies, and democracies sanction authoritarian actions. Germany and the EU have become targets of the right-wing populist Prawo i Sprawiedliwość (PiS/Law and Justice) government in Poland. The current government has sought to expunge any guilt the “Polish Nation” incurred during the Second World War by engaging in an aggressive revisionist campaign aimed at denying Poland’s participation in Nazi death camps.

Furthermore, Poland’s attempt to sack its Constitutional Court and replace 27 justices with PiS loyalists has alienated it from France, Germany, and the European Commission, which opened an Article 7 investigation last year into Poland’s actions and is currently threatening to take legal action against it. Likewise, Hungary has taken an antagonistic stance with EU members and their efforts to promote rule of law. Budapest has been in an entrenched battle against the EU, in what Orbán has called “liberal forces acting against Central and Eastern European countries,” while actively opposing and restraining EU laws on immigration, entertaining anti-Semitic conspiracy theories, and curtailing individual freedoms within Hungary’s borders. The right-wing populism of both Poland and Hungary, with their villainization of minorities, suppression of dissent, crackdown on civil society, and erosion of democratic norms and institutions, puts them at odds with their NATO allies and EU partners, fostering uncertainty and deep mistrust among them.

#### Trump’s legacy of anti-NATO sentiment decks American credibility within NATO and European policy writ-large

Nicholas **Burns 18,** Professor of the Practice of Diplomacy and International Relations at the Harvard Kennedy School, former NATO ambassador. “"NATO at Seventy: An Alliance in Crisis," Belfer Center for Science and International Affairs. 10-19-2018, , https://www.belfercenter.org/publication/nato-seventy-alliance-crisis, accessed 6-21-2022//cpd

Challenges from Within NATO

Reviving American Leadership of the Alliance

NATO’s single greatest challenge is the absence of strong, principled American presidential leadership for the first time in its history. President Donald Trump is regarded widely in NATO capitals as the Alliance’s most urgent, and often most difficult, problem. NATO leaders, for example, considered not holding a 2019 summit to mark the seventieth anniversary this spring as they did in decades past. They feared President Trump would blow up a meeting in controversy as he has done each time he has met with NATO leaders during the past two years. Wary of his past behavior, NATO plans a scaled down leaders meeting for December 2019.

President Trump’s open ambivalence about NATO’s value to the U.S., his public questioning of America’s Article 5 commitment to its allies, persistent criticism of Europe’s democratic leaders and embrace of its anti-democratic members and continued weakness in failing to confront NATO’s primary adversary President Vladimir Putin of Russia, have hurtled the Alliance into its most worrisome crisis in memory.3

There is no reason to believe President Trump’s attitude will change for the better during the next two years. He believes NATO allies are taking advantage of the U.S.4 These are the same allies and partners who came to America’s defense on 9/11, suffered more than 1,000 battlefield deaths alongside American soldiers in Afghanistan,5 are fighting with the U.S. now against the Islamic State and shoulder the main burden sustaining a fragile peace in the Balkans, in both Kosovo and Bosnia and Herzegovina.

President Trump is the first U.S. president to view the European Union as an economic competitor rather than a vital partner of both the U.S. and NATO. His troubling anti-NATO and anti-Europe bias has caused European governments to question the credibility of the U.S. as the leader of the West for the first time since the Second World War.6 The European public confidence in American leadership is also at historically low depths.7 Every American president before Trump has encouraged the strength and unity of Europe as a core interest of the U.S. Trump may well cause even greater damage to the Alliance while he remains in office.

For this reason, Republicans and Democrats in Congress must act together as a blocking force against President Trump’s dangerous policies. Congress, on a bipartisan basis, should reaffirm the U.S. commitment to the Article 5 defense clause in the NATO Treaty. Congress should pass legislation this year requiring Congressional approval should President Trump attempt to alter U.S. treaty commitments to NATO allies or to have the U.S. leave the Alliance altogether.8 Congress should continue to fund the “European Deterrence Initiative” to bolster U.S. military strength in Europe that is the primary deterrent against Russian adventurism.

### 2nc – turkey not k2 nato – general

#### Turkey’s NATO participation does more harm than good

Antoine **Got**, 11-19-20**20**, "Turkey’s Crisis with the West: How a New Low in Relations Risks Paralyzing NATO," War on the Rocks, https://warontherocks.com/2020/11/turkeys-crisis-with-the-west-how-a-new-low-in-relations-risks-paralyzing-nato/, accessed 6-23-2022//cpd

NATO’s most important challenge today may not come from Russia, but from within. With the number of disputes between Turkey and several European allies yet again on the rise, the two parties’ souring relations have begun undermining the organization’s cohesion and ability to make timely collective decisions. If left unaddressed, these tensions could cause serious damage to the world’s most powerful alliance.

The latest flashpoint came from Turkey’s open backing of Azerbaijan’s war effort in the small landlocked enclave of Nagorno-Karabakh, which ended abruptly in early November thanks to a Russian-brokered deal. Reports of military assistance and alleged Syrian mercenaries sent by Turkey placed Ankara at loggerheads with its NATO allies’ calls for a peaceful, negotiated resolution to the conflict. The deal, which foresees Baku reacquiring sizeable portions of the disputed enclave, has made Turkey one of the obvious winners of the recent flare-up, while its Western allies remain on the sidelines. For some, this could be the straw that breaks the camel’s back, adding to a long list of complaints they have recently leveled against their NATO ally.

BECOME A MEMBER

Last month, Greece and Turkey came dangerously close to a head-on naval confrontation in disputed Eastern Mediterranean waters over Turkey’s gas exploration activities near the Greek island of Kastellorizo, just a few hundred meters away from the Turkish coast. Though Turkey later withdrew its ship, tensions between the two NATO allies spiked again following Turkey’s announcement that it would send the ship back for a 10-day seismic research mission in the area, renewing Greek calls for sanctions. What makes this a particularly explosive situation, of course, is the two Eastern Mediterranean powers’ lingering dispute over the post-1974 division of Cyprus and the discovery of energy resources in the area.

A similar confrontational encounter occurred in June when France and Turkey nearly came to blows after a French warship, the Courbet, tried to inspect a Turkish vessel for allegedly breaching a U.N. arms embargo on Libya — a claim Ankara fiercely denies. Supporting different sides in the Libyan Civil War, the two allies have been engaged in a war of words over each other’s provocative deeds in the Libyan, Syrian and Nagorno-Karabakh conflicts, as well as over Turkey’s territorial claims in the Mediterranean. The latest spat followed President Emmanuel Macron’s defense of a cartoonist’s right to caricature religious figures in the wake of a teacher’s beheading, to which Turkish President Recep Tayyip Erdoğan responded by calling for a boycott of French products.

Within NATO, the escalation in tensions and growing entanglement of the two camps’ now numerous disputes reflects European allies’ mounting frustration over what they perceive as Turkey’s self-serving and aggressive regional posturing, and its unwillingness to consult allies before acting. A NATO member since 1952, Turkey has always occupied a somewhat unique role in the alliance. Its size, military resources, and key position at the doorstep of Asia — in other words, as NATO’s southern flank — give it important strategic relevance within the context of renewed interest in the Middle East. Though relations have often been fragile, especially since the 2016 coup attempt, the current rift marks a new low in the recent history of the alliance, with potentially damaging consequences. Given this backdrop, NATO should take advantage of its own resources to try to address its members’ deteriorating relations, and work to reconcile their diverging security interests. This is a lot easier said than done, but it may be the only option to prevent a more fundamental rupture in the relationship.

Divided We Stan

As tensions grow, a key risk for NATO relates to the crisis’ potential to hamper its cohesion and ability to act decisively, as the alliance relies on the principle of consensus to successfully operate. Every major NATO decision embodies the collective will of all allies and results, therefore, from a complex but fragile process of negotiation wherein nations are invited to compromise on matters of mutual interest. The inevitable drawback to this is that every ally possesses a de facto right to veto any NATO issue if its demands are not met, which they may be incentivized to use as leverage to pursue national interests. The same can be said of the European Union, which operates on unanimity and where Cyprus recently made headlines for blocking sanctions on Belarusian President Alexander Lukashenko’s regime, insisting on the imposition of E.U. measures on Turkey for its energy exploration in Mediterranean waters. The European Union was criticized for failing to agree on timely sanctions.

Unlike the European Union, NATO consultations are held behind closed doors, and disagreements largely avoid public scrutiny. In principle, however, any nation’s objections could stall key alliance policy or business. Last year, leaks revealed that Turkey had threatened on the eve of a NATO summit to block a key defense plan to protect the Baltic states and Poland against Russian aggression unless NATO backed its own recognition of the Kurdish People’s Protection Units militia as terrorists. Likewise, for years, Turkey had vetoed NATO cooperation with neutral Austria under its partnership program in response to Vienna’s calls for the European Union to halt membership talks with Ankara. Though in both cases deals were eventually reached to break the deadlock, and though such negotiation tactics are not uncommon, these incidents highlight a mounting climate of uncooperativeness and unwillingness to compromise between allies, making interaction increasingly difficult.

As Ankara grows more defiant, NATO members are indeed finding it difficult to reign in their southeastern ally. With the 2011 Arab Spring and its aftermath, the rapid deterioration of Turkey’s regional and domestic security environments has coincided with a growing perception that its Western allies are not giving enough credence to its core security interests. The stalled European Union membership project, together with America’s disengagement from the Middle East, support for the Kurdish People’s Protection Units militia, and persistent refusal to extradite cleric Fethullah Gülen, the presumed mastermind of the failed 2016 coup attempt, have all contributed to strengthening the conviction that Turkish security interests are likely best served through autonomous action — and not by relying on a suspicious and divided West. This impression is reinforced by Europe’s vocal criticism of Erdoğan’s concentration of executive power, and by the country’s worsening economic and social woes.

Overall, these factors have eroded NATO’s credibility and influence over Ankara, just as the latter has become more conscious of its own considerable leverage over Europe due to its key role in Syria, which NATO sees as the defense of its southern frontier, and in easing the pressure to accommodate large arrivals of refugees on European shores. The former is linked to Turkey’s vetoing of NATO’s defense plan for Poland and the Baltics, which aimed at compelling NATO to provide greater support in Turkey’s defense of the alliance’s southern flank — something Ankara has demanded for years. Likewise, Turkey’s handling of its four million-strong refugee population, the largest in the world, has contributed to Ankara’s influence over Brussels through its instrumentalization of fears that it would “open the gates” to Europe for migrants and refugees, which Erdoğan announced earlier this year in violation of a 2016 E.U.-Turkish agreement. Given its shrewd sense that the tables have turned, Ankara has lost many incentives to cooperate. Of course, one key risk is that Turkey’s bold strategy backfires and leads to a fresh round of retaliatory measures such as collective sanctions or cutbacks in E.U. funds, with damaging effects on Turkey’s weakening economy.

For NATO, another conceivable consequence lays in the reinforcement of calls for greater European “strategic autonomy” in the realms of defense and security, with potentially harmful repercussions on the future of the transatlantic community. Against a backdrop of deteriorating Euro-Atlantic relations, several leaders have begun to publicly question the relevance and effectiveness of NATO as an organization. A staunch advocate of the “strategic autonomy” concept, Macron reacted to the clash with Turkey over the arms embargo on Libya by reiterating his assertion that NATO was “brain dead” for being unable to temper Turkish adventurism. In a recent interview, Armenian President Armen Sarkissian echoed these remarks by putting at stake NATO’s credibility over the organization’s seeming inability to influence its member’s involvement in the Caucasus. Were NATO to become increasingly paralyzed by souring internal relations, doubts about the effectiveness and reliability of the organization could further incentivize E.U. countries into acting beyond the NATO framework. Regrettably, this could result in accelerating E.U. states’ ostracizing of Ankara, while persuading some allies into seeking additional bilateral arrangements as more reliable forms of security guarantees.

E.U.-Turkish tensions have also brought to the fore Ankara’s ambiguous ties to Moscow. Though relations hit rock bottom over the downing of a Russian Su-24M fighter jet in 2015, the two countries have since rebuilt extensive political and economic ties, culminating with high-profile endeavors such as the TurkStream pipeline and Ankara’s 2017 purchase of a Russian S-400 surface-to-air missile defense system. The moves drew stern condemnation from Washington and other NATO allies, with some going as far as to label them as signs of a Turkish pivot to the East. What made this rapprochement all the more alarming were the two countries’ ostensible affinities over their highly centralized, authoritarian-leaning political systems, which run counter to the core values of the alliance. The main fear is that these newfound affinities introduce vulnerabilities within the alliance through bilateral ties that Moscow can exploit to drive Turkey further away from the West, and sow division to weaken NATO’s ability to act.

### 2nc – turkey not k2 nato – sweden/finland

#### Turkey makes political issues conditional – Sweden proves

Associated **Pres**, 5-25-20**22**, "Turkey Demands 'Concrete Steps' to Back Nordics' NATO Bids," US News & World Report, https://www.usnews.com/news/business/articles/2022-05-25/sweden-finland-delegations-in-turkey-for-nato-talks, accessed 6-24-2022//cpd

Kalin said Turkey’s proposal to lift arms export limits was met with a “positive attitude” by the Swedish and Finnish delegations. He added that talks would continue once the Nordic governments had responded to Turkey’s demands. Turkey also expects the extradition of 28 “terrorism” suspects from Sweden and 12 from Finland, Kalin said, adding that there was “no legal or judicial basis” not to extradite them. Turkish state media had previously said Turkey demanded the extradition of 33 suspects from the two countries. Swedish Prime Minister Magdalena Andersson said following a meeting with European Council President Charles Michel in Stockholm that her country wanted to “clarify” claims that have been floating around during discussions with Turkey. “We do not send money or weapons to terrorist organizations,” Andersson said. During a news conference with the Estonian prime minister later Wednesday, Andersson said that “in these times, it is important to strengthen our security.” She said Sweden has “a constructive dialogue” with Turkey and that Stockholm was “eager to sort out issues and misunderstandings and questions.” Michel, who is scheduled to head to Helsinki from Stockholm, said it was “a pivotal moment for Sweden" and “we fully support your choices.” Turkey this week listed five “concrete assurances” it was demanding from Sweden, including what it said was “termination of political support for terrorism,” an “elimination of the source of terrorism financing,” and the “cessation of arms support” to the banned PKK and a Syrian Kurdish militia group affiliated with it. The demands also called for the lifting of arms sanctions against Turkey and global cooperation against terrorism. Turkey said that it has requested the extradition of Kurdish militants and other suspects since 2017 but hasn’t received a positive response from Stockholm. The Turkish government claimed Sweden had decided to provide $376 million to support the Kurdish militants in 2023 and that it had provided them with military equipment, including anti-tank weapons and drones. Finland has received nine extradition requests from Turkey in a recent period covering over three years, Finnish news agency STT said Wednesday, citing data from the Finnish justice ministry. Two people were extradited while six of the requests were rejected. A decision was pending regarding one other case.

### 2nc – nb – digital authoritarianism

#### Global digital authoritarianism greenlights Chinese and Russian aggression- turns the aff

Justin **Sherman** 20**21** “Digital Authoritarianism and Implications for US National Security.” The Cyber Defense Review, vol. 6, no. 1, 2021, pp. 107–18. JSTOR, [https://www.jstor.org/stable/26994115. Accessed 24 Jun. 2022](https://www.jstor.org/stable/26994115.%20Accessed%2024%20Jun.%202022).//cpd

Private firms worldwide legally or illegally have long been selling dual-use digital technologies that can be used to monitor web traffic and to censor information. That there is a global market for digital surveillance tools is old news. Companies incorporated in democracies heavily export these dual-use technologies worldwide, including, in many documented cases, to despots.[12] Likewise, companies incorporated in autocracies sell dual-use technologies, including those that can be used for censorship and surveillance, to other authoritarian regimes.[13] Some studies suggest that democracies account for a far greater volume of surveillance technology exports, including to despots, despite attempts to restrict such exports.[14] The pursuit of digital authoritarianism to bolster state power magnifies incentives for some countries to acquire dual-use surveillance tools, and for others to encourage their spread. China’s state leadership, for instance, consistently has advocated a sovereign and controlled Internet governance model on the global stage, with practices like censorship and surveillance, as opposed to a global and open model supported by many liberal democracies.[15] In tandem with this global diplomatic messaging, the Chinese government has reportedly conducted trainings on new media or information management with representatives from dozens of countries, many on record as pursuing restrictive online practices.[16] This has coincided with countries targeted by the Belt and Road Initiative passing cybersecurity laws that sometimes mirror laws already enacted in China, such as Vietnam’s recent establishment of data localization requirements.[17] Causality remains unclear in this situation, and empirical questions remain to be answered about the underlying drivers of digital authoritarianism in different countries. Nonetheless, these patterns and events, coupled with exports of surveillance technologies from China, raise questions about Beijing’s intentions to spread digital authoritarianism globally, including through a greater focus on, and/or endorsement of, the sale of digital surveillance and control capabilities. This could amplify the aforementioned national security risks, should authoritarian countries acquire the tools and/or knowledge needed to bolster their power through digital surveillance. National security analysts have already flagged these potential risks across Africa. Many countries China has engaged with through its Belt and Road investments have acquired Chinese surveillance technology, potentially usable for oppressive purposes. For instance, Chinese company exports of surveillance technology to the Ethiopian government have occurred alongside Chinese government investments.[18] Given China’s history of spying on and suppressing political dissidents, this is hardly a benign fact, and Ethiopia is but one of several examples. Should China’s leadership be intent on spreading digital authoritarianism worldwide, to include diffusion of surveillance tools, this likely could include countries aligned with China’s national security and/or economic interests. Like China, Russia has long advocated for cyber sovereignty on the international stage,[19] with President Vladimir Putin repeatedly emphasizing the importance of information control within a country’s sovereign borders.[20] As noted above, Russian companies export surveillance and hacking technologies, especially to post-Soviet states.[21] Andrei Soldatov and Irina Borogan actually suggest that Russian surveillance technology exports to some of these countries are a better fit than Western-made surveillance applications, because Russian laws and procedures governing traffic interception are more compatible for these countries, and the technologies are tailored accordingly.[22] In either case, these surveillance technology exports need further study, and they clearly serve as tools of political influence in Russia’s near-abroad. As with China, the extent of the Russian government’s direct involvement in and support of such exports needs further study, because the Kremlin’s direct hand in these exports, while visible, is hardly transparent. The desire to spread digital authoritarianism may well incentivize the Kremlin to better spread its surveillance technologies, or to at least look the other way when they occur, and thereby consolidate power in the hands of Russian-aligned countries at the expense of US government interests. This also could threaten vulnerable democracies worldwide, and facilitate the so-called fracturing of the global Internet, as countries build out technical and legal regimes that filter the global and open Internet touching and running through their borders.[23] Again, the threat here is not only from governments in China and Russia. Companies incorporated in democracies also sell a high volume of dual-use surveillance technologies to despots, and this is something we are better able to monitor and correct. It is also important to reemphasize the existing incentives for countries to encourage or allow the spread of these capabilities to other countries (including the technologies and how to optimize them). But growing desires to spread digital authoritarianism globally not only undermine human rights and developing democracies; this also exposes US national security to increased risk.

## Pilot PIC

### 1nc – cp

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

---dcp is textually and functionally severance

--perm do both links to net benefit – pilot projects cause centralization

#### The plan institutionalizes and exports the DoD’s AI bureaucracy internationally – preventing direct feedback loops and effective operationalization of AI for mission-critical requirements

Marc Losito & Anderson 21, John Anderson, Marc Losito is a first-year Master of Public Policy candidate at Duke University and an active-duty U.S. Army Warrant Officer, focusing on the intersection of technology and national security policy. Marc holds a degree from Norwich University and has served in the military and Special Operations Forces for 20 years specializing in counterterrorism, irregular warfare, and intelligence operations. John Anderson is a U.S. Army Reserve military officer focused on applying AI and machine learning to mission critical problems. He has served in the U.S. Army for nearly 20 years and previously worked in the financial industry as a senior research analyst at a value-oriented hedge fund and a mid-sized private equity firm. He holds degrees from the University of North Carolina at Chapel Hill and Columbia Business School. 5-10-2021, "The Department of Defense’s Looming AI Winter," War on the Rocks, <https://warontherocks.com/2021/05/the-department-of-defenses-looming-ai-winter/>, nihara

The Four Horsemen of the Department of Defense’s Looming AI Winter

The four horsemen of the forthcoming AI apocalypse, so to speak, are this time around human problems without technological scapegoats. They are a lack of AI expertise, too much AI bureaucracy, the challenge of democratizing AI to the user level, and an old-fashioned approach to AI integration.

Domain Expertise: The Education Challenge

To become an AI force, the Department of Defense should inculcate AI domain expertise at appropriate levels of leadership — with the warfighters who employ AI, not bureaucrats. Creating a curriculum for AI within enlisted and officer professional military education should be a priority. The curriculum should include a breakdown of the core components of an AI pipeline — data, computing, algorithm development, test/evaluation, and AI-enabled platforms.

Commanders and their staff should have AI Smartcards, a rubric for exercising domain expertise, at the ready. First introduced in February 2021, the smartcard is structured into six main categories corresponding to the core functionality comprising an AI system. The smartcard is a framework for curriculum, both readily adaptable for professional military education learning modules and unit-level adoption. Not simply a technical guide, the AI Smartcard also helps the unit to think through operationalizing AI and becoming “AI-ready.”

An indicator that the scales are being rebalanced will be warfighters peppering AI subject matter experts with questions that get to the heart of the smartcard — is real AI being delivered? When slick briefings full of drive-by tech-splanations of AI capability evolve into a user asking penetrating questions to get the heart of AI performance, then the expertise obstacle will have been overcome.

Bureaucracy: The Management Challenge

Bureaucracy can be a beautiful thing — structure, talent, mission, and resources coming together in a cohesive, logical manner to deliver mission-critical capabilities. With that said, Department of Defense bureaucracies have a way of calcifying around programs and people, not actual capabilities. The consequence of the AI bureaucracy — which consists of several one-off groups organized around the task of bringing AI to the department, but which are stovepiped away from the people they’re actually trying to buy AI for — is an unnecessary buffer between users and developers. This convoluted system confuses what should be a direct feedback loop to ensure that capabilities are acutely focused on mission-critical requirements.

The department should shrink centralized groups like the Joint AI Center and the Army Futures Command AI Task Force and instead send their authorities, decision-making power, and resources down to operational units. AI centers of excellence should be creating processes, policies, and resourcing to facilitate a constant feedback loop between user and developer, with no-one in between to garble the message. They should exist as idea-centric organizations at the service level that cut across the warfighting functions, providing the tools, lessons learned, resources, and expertise to help commanders to operationalize AI. The bureaucracy should connect intent, constraints and restraints, and resources — and then get out of the way.

The Department of Defense’s managing philosophy with respect to AI bureaucracy should mirror the computer programming concept called the “self-deleting executable.” It is a string of code designed to allow a program to delete itself. Instead of thinking in terms of hiring hundreds of pseudo-experts, think in terms of creating an organization and then setting an egg timer for it to expand and contract, responsive to a direct user-developer feedback loop. The AI bureaucracy only survives as a platform to connect users with development talent, contracting, and computing power. It should shrink, not expand, over time.

#### Pilot projects prevent AI integration at scale – no robust pipeline for innovation – AND, ties cost estimates to legacy systems which consolidates bureaucratic centralization and guarantees AI failure

Marc Losito & Anderson 21, John Anderson, Marc Losito is a first-year Master of Public Policy candidate at Duke University and an active-duty U.S. Army Warrant Officer, focusing on the intersection of technology and national security policy. Marc holds a degree from Norwich University and has served in the military and Special Operations Forces for 20 years specializing in counterterrorism, irregular warfare, and intelligence operations. John Anderson is a U.S. Army Reserve military officer focused on applying AI and machine learning to mission critical problems. He has served in the U.S. Army for nearly 20 years and previously worked in the financial industry as a senior research analyst at a value-oriented hedge fund and a mid-sized private equity firm. He holds degrees from the University of North Carolina at Chapel Hill and Columbia Business School. 5-10-2021, "The Department of Defense’s Looming AI Winter," War on the Rocks, <https://warontherocks.com/2021/05/the-department-of-defenses-looming-ai-winter/>, nihara

Integration: The Iceberg Challenge

The Department of Defense’s initial glimpse of AI led it to believe it could develop or buy AI on the cheap and integrate it with existing programs of record as a bolt-on. These assumptions were ill-conceived. For example, the Air Force experienced some initial success with integrating AI into the Distributed Common Ground System, but then realized the one-by-one “AI decision aids” are “single point demos” as opposed to AI at scale. AI worthy of near-peer competition is expensive, and should be integrated into systems built with AI in mind, from the ground up.

Since 9/11, the Department of Defense has been engaged in near-constant combat against violent extremist organizations across the globe. In this fight, warfighters achieved mission success almost in spite of the digital tools provided to them. Microsoft PowerPoint, not AI, could still win the day. Commanders and warfighters haven’t had the time or wherewithal to provide the feedback necessary to blow up the first-generation digital tools and software fielded by programs of record. Troops just compensated for the existing tool or purchased commercial off-the-shelf tools without going through the hassle of dealing with the bureaucracy.

The department’s development and acquisition machine — programs of record, program executive offices, requirements specialists, acquisition professionals — never got the message of how truly rotten and eroded the warfighter’s underlying digital foundation had become. Seeing the initial fielding of commercial AI to the warfighter, the same programs that have failed in the past now assume “we too can do this,” rolling out buzzwords like “AI-ready” or “AI-enabled” — and asking for more money to build their own AI on the cheap, anchoring their cost estimates and requirements on the same failed legacy programs. In this mass of confusion, it’s difficult to distinguish between “drive-by AI” and real, enduring capabilities. The Department of Defense is falling for the former. Drive-by AI is best characterized as one-off pilot projects without a robust AI pipeline — data, data labeling, computational power, algorithm development, test and evaluation — integrated on legacy tools that don’t allow users to continuously feed back existing and new use cases for the AI.

### decentralization good

#### Centralization of AI development causes extensive oversight that destroys operability in contemporary battlefield environments AND multi-domain operations – BUT, institutionalization of decentralized approaches to tech development guarantees NATO primacy – CPs development approach is exported globally

-- VUCA = volatile, uncertain, complex, and ambiguous

Col Mark C. Boone 21, Col Boone is currently serving as the Deputy Chief of Staff, Marine Forces Europe/ Africa and is a first-year PhD student at the University of Charleston, WV, where he studies executive leadership. November 2021, “Decentralized Decision Making: A paradigm-shift in thinking for NATO and future U.S. alliances in the Asia-Pacific region,” Marine Corps Gazette, <https://mca-marines.org/wp-content/uploads/67-Decentralized-Decision-Making.pdf>, nihara

The 21st century has ushered in an era of intense technological advancement, changing the character of warfare. Hypersonic weapons, autonomous platforms, ubiquitous sensors, big data, quantum science, additive manufacturing, and artificial intelligence are but a few of the technological developments changing the landscape of the world and warfare as we know it. The conduct of warfare, from its fundamental principles to ethical framework, is being challenged.

As state and non-state actors alike strive for overmatch in this technological arms race, the West, namely the United States along with its fellow NATO allies, currently possesses the human resources required to develop, maintain, and hone overmatch at all levels of warfare. The West can ensure intellectual overmatch by fostering a culture of decentralized decision making where a relationship of trust and mutual understanding exists between leaders at all levels. It is based upon understanding “intent” and where the encouragement of subordinate-driven initiative and decentralized decision making at all levels is expected.

This requires a revolution in thinking, a paradigm shift institutionalized across the NATO enterprise. Change must occur across our institutions from our entry training to our career professional development and unit certification processes. A culture of kinship, trust, and mutual respect among leaders at all levels needs to be revitalized. If NATO can do this, true primacy will be gained at all levels of warfare resulting in speed, tempo, and battlefield lethality far surpassing our adversaries. As the DOD—namely the Marine Corps— approaches capacity and alliance building throughout the Asia Pacific, this same developmental calculus must be considered. Time, space, and disaggregated operations throughout this region will require decentralized decision making of the highest order. Long standing partnership such as Australia will be well suited to make this paradigm shift; however, emerging security partners, such as Vietnam and India will require substantial assistance in technological development and mindset.

The Battlefield of the Future

Future battlefields will be volatile, uncertain, complex, and ambiguous (VUCA).3 They will be trans-regional, multi-functional, and multi-dimensional, requiring enhanced joint interoperability well inside the adversaries’ weapons engagement zone.4 Communications will be degraded, the massing of any assets or personnel will be costly, and all domains, air, land, sea, cyber, and space will be contested.5 Massive convergence of capabilities in time and space across all domains, physical and non-physical, will be required. Electromagnetic signature reduction will become the new art of camouflage and immediate combat decisions will be made through sheer instinct, frontline analysis, and most importantly, a clear understanding of mission objectives. “Commanders intent” will rule the day.

Hooked on Technology

After nearly two decades of counterinsurgency (COIN) centric conflict in the Middle East, the United States has an entire generation of officers, many now senior, who have grown quite dependent on technology. An operational environment of airspace dominance, instantaneous access to information, uninterrupted communications, and the unblinking eye of unmanned platforms providing realtime battlefield imagery has created a generation of leaders with an insatiable appetite for information.7

Worse, this environment has eroded our decentralized decision making. Decisions are now made levels above where they should be because of the technological ease of involvement and a desire for absolute precision. When senior officers step down from the strategic or operational levels of warfare into the tactical, they create resentment, a lack of trust, uncertainty amongst subordinate leaders, and an environment of dependency.8

The problem of technologically driven command and control (C2) and decision making has been further exacerbated through the application of COIN principles during the last two decades of operations. COIN involves significant measures to embrace the local population with strict avoidance of collateral damage. Avoidance of unnecessary civilian casualties and protection of noncombatants are principles of warfare enshrined in International Humanitarian Law and the Geneva Conventions; however, COIN application took these principles to levels unforeseen before in warfare resulting in constriction of authorities, reduced subordinate initiative, and direct involvement and oversight by senior commanders in tactical operations with suboptimal results.

This has resulted in an overly centralized command philosophy where decisions are made after massive data analysis to examine all exigencies, thus stifling subordinate initiative and development.9 Under the auspices of these unrealistic expectations, the targeting authority for lethal actions has been removed from the operator and restricted to upper echelon decision makers. Decisions that should be made by captains are now being made by colonels. Precious time is lost when the targeting decision cycle requires approval from a hierarchal chain of command.10 The future VUCA environment will not permit this manner of operations. Approval authority for kinetic and non-kinetic fires will need to be maintained at battalion, company, and at times squad level.

Auftragstaktik: A Philosophy of the Art of War and Leadership

At the turn of the 19th century, the Germany Army developed Auftragstaktik, a new philosophy for waging war. Designed to enhance speed of action, Auftragstaktik was refined during the internal struggles of trench warfare in World War I, resulting in the operational concepts of the elastic defense in 1916 and the assault tactics of 1918. Following the war, these concepts were further developed in the German Army Field Manual of 1933, which promoted the aggressive Blitzkrieg tactics of World War II.12

Auftragstaktik was not simply the issuance of mission command orders, a C2 system, or laissez-faire free for all. It was a way of thinking, encompassing an understanding of warfare, leadership traits to be exemplified, C2 mission command orders, and an emphasis on relationships. This new way of thinking was institutionalized through the training and education of the entire force, introduced during basic training, and continued throughout their careers. Leaders at all levels embraced these groundbreaking concepts and developed a professional kinship based on trust and knowledge of each other’s abilities.13

Auftragstaktik was a broad-based institutionalized philosophy encompassing the art of warfare, the strength of which was anchored in relationships. Relationships based upon mutual trust, keen insight into each other’s abilities, and respect amongst warriors. It was an environment where commanders at all levels developed the “what” of commander’s intent with the expectation that subordinates would exercise the full scope of their initiative, experience, intellect, and ingenuity to derive the “how” of mission accomplishment.14

Subordinate driven action and decision making was not just expected; it was an institutional vow. Mistakes were expected and corrected as part of professional development, while inaction or indecisiveness was not tolerated.15 Critical thinking and a joy of responsibility were derivatives of self-generated discipline, and the Germans understood the importance of operating one up and thinking two down.16 Auftragstaktik created a culture of decentralized decision making with a universal understanding that no operational plan survived contact with the enemy and a belief that every action in combat is unique, requiring initiative, rapid assessment, and aggressive action.17

Developing a Culture of Decentralized Decision Making

Since World War II, several American military organizations have attempted to replicate the theory of Auftragstaktik. The Army has made strides with its development of Mission Command and the Adaptive Leadership Training and Education model focused on problem solving skills and critical thinking; however, neither have been institutionalized across the force.19 The DOD pioneered the “Joint All Domain Command and Control System” to enhance decision making at lower levels, but this concept is still embryonic.20 The Marine Corps, renown for adaptability and emphasis on their NCO leadership, has released MCDP 7, Learning, outlining a visionary philosophy where the mind is the weapon surpassing all forms of technology.21 Despite these measures, the overall focus across the joint force remains on centralized decision making.

The true spirit of Auftragstaktik, understanding “intent,” the inherent relationship between leaders, and the delicate balance between authority and responsibility, has been overlooked and has not been institutionalized in U.S. military training centers and universities. A complete paradigm shift in thinking is required in our teaching methodologies from “what to think” to “how to think.” A cognitive leap must be made from competency-based learning to outcome-based learning. Our training institutions must shift from report card box-checking to discovery learning and development. This change must cover the entire educational spectrum from our entry-level training to our seniorlevel professional development and must be institutionalized in our training centers for deployment and combat readiness.22 Additionally, this must include joint multi-domain exercises in a C2 denied environment, challenging and stress checking our processes, equipment, and people.23

Emotional intelligence must be a key attribute of leadership allowing for subordinate level involvement in decisions and outcomes. We need to instill the importance of developing deep and enriching professional relationships throughout the force, relationships developed through shared hardships, rigorous real-world training, and in places like the officer and staff-NCO clubs, where tactics and life lessons are shared from teacher to scholar.

The King of Domains: The Human Domain

Message to the Joint Force 2015

Critics argue that decentralized decision making and mission command are dying concepts. An argument is made that technological advancements in artificial intelligence, quantum computing, and big data analysis will overcome the need for critical thinking and human decision making on the battlefield. Leaders will be replaced by machines, and fighting will be done largely by unmanned platforms.25 History will prove them wrong. History is already replete with The inventions of today and tomorrow will create a new paradigm in warfare, one in which the Sailor, Soldier, Marine, or aviator—enabled by technology—will still be required to make decisions.27 We currently have the domains of sea, air, land, cyber, and space; however, the human domain reins above all. Future warfare will be faster, more lethal, and more dispersed than ever witnessed before. Leaders at all levels will operate off instinct and commander’s intent in an environment of degraded communications, cloaked identification, strained supply lines, and extremely dispersed formations. The emergence of new weapons with significant range and lethality will require forward unit control. In this environment, decentralized decision making will become even more paramount and small unit leaders at the company and squad level will require operational authorities historically maintained at the brigade level and higher.

Undoubtedly, to assist leaders, emerging technologies to enhance decision- making processes should be explored and utilized. Technologies, such as the Defense Advanced Research Projects Agency Deep Green, a system to enter into the adversarial decision-making process or the Real-Time Adversarial Intelligence and Decision Making, which uses predictive analysis and simulations to analyze enemy actions, should be further analyzed.28 Another emerging technology to enhance decision making is Think, Analyze, and Connect, a massive search engine for analysis being implemented by the Defense Threat Reduction Agency for collaboration and decision making.29 The Joint Assistance for Deployment Execution, designed for planning and course of action comparison, is yet another within this family of systems.30

With the emergence of the Global Information Grid, everyone now has access to the same data. Senior leaders, non-natives to the digital era, are at a distinct disadvantage. Anyone harboring information at higher echelons will quickly become irrelevant and part of the problem.31 Knowledge is only powerful if it is shared and sharing information must be viewed as a way to enhance decision making amongst subordinates. The German model of Auftragstaktik placed emphasis on the tactical commander for flexibility in making decisions to affect the overall intent.32 Technology should not be used as a means to micromanage but to enhance our subordinates’ ability to observe, orient, decide, and act faster than our enemy.33

Now, in an era of advanced technologies with the potential to create over supervision, more emphasis must be placed upon the issuance of clear and concise commander’s intent, the sinew between the mission and the concept of operations.34 Decentralized decision making is the only way to harness the collective energy of the joint force enhancing lethality and survivability on the modern battlefield. The concept of the “Strategic Corporal” is still valid and needs to be rekindled.35 At the same time, we must focus the development of our senior leaders on the strategic application of all instruments of national power, critical thinking, and the art of enabling decentralized decision making by their subordinates.36

Enabling the Paradigm Shift

Much has been written about the future of warfare. We know it will be trans-regional, multi-domain, and multi-functional. New technologies will emerge altering the very character of warfare and victory will go to those who harness the chaos of the VUCA environment using speed and tempo to enhance their lethality. The future battlefield will require decentralized decision making with operational authority pushed to the lowest level possible. In this complex and volatile environment, NATO can establish and maintain strategic and operational primacy over our adversaries through investment in our human capital. To achieve this, NATO must revolutionize the way we think from “what to think” to “how to think.”

This radical change must be institutionalized across the force from the onset of training through career progression. Training must be challenging, setting conditions for a real-world experience where all domains are contested. It must stress test our people, equipment, and processes to ensure operational readiness and resilience.

What the Alliance needs is a new culture of Auftragstaktik where commanders develop true relationships with their subordinates, a culture where the commander’s intent is the watch word of operations, and where the “how” of mission accomplishment is left to subordinates. We must foster an environ- ment where our subordinates know to take action in the absence of orders. We must train to an expectation of initiative and encourage them to employ their ingenuity, experience, and knowledge of the environment to ensure that the commander’s vision becomes a reality.

### multidomain operations

#### Effective cross-domain strategies is key to deterrence of grey-zone strategies in land, air, sea, cyber, and space

Sweijs, T., Zilincik 21, S. 2021, The Essence of Cross-Domain Deterrence. In: Osinga, F., Sweijs, T. (eds) NL ARMS Netherlands Annual Review of Military Studies 2020. NL ARMS. T.M.C. Asser Press, The Hague. <https://doi.org/10.1007/978-94-6265-419-8_8>, nihara

Deterrence is about convincing adversaries to refrain from certain behaviour through the prospect of costs that outweigh the benefits.1 As related in the preface to this volume by Osinga and Sweijs, deterrence has been a central tenet of strategic practice throughout history,2 even if its logic was only clearly articulated in the aftermath of the Second World War. Deterrence scholarship has since then evolved in four consecutive waves. The first, second and third wave of the deterrence literature, which emerged during the Cold War, tended to almost exclusively focus on deterrence of high-intensity aggression including most importantly the possible use of nuclear weapons alongside large scale conventional invasion.3 Lower-intensity threats which were considered mere nuisances were largely left outside of the scope of investigation.4 However, these became more important in the 1990s with the demise of the Soviet Union and the emergence of non-traditional threats such as terrorism.5 This gave birth to the fourth wave of deterrence literature that focused on the question whether deterrence would work against such threats that emerged in the 1990s and 2000s.6 Over the past decade, a new body of ideas has been emerging concerning the application of deterrence in today’s strategic environment. An important characteristic of our age is the proliferation of ways and means by which hostile activities can be perpetrated. Accordingly, strategists have started to pay more attention to the application of deterrence in new domains and to cross domain deterrence (CDD), across both traditional and new domains. This chapter appraises the contribution of the emerging body of cross domain deterrence literature to deterrence theory and deterrence practice. It explains the context in which theories of cross domain deterrence have emerged and elaborates different conceptualisations of cross domain deterrence distinguishing between two different approaches. The conclusion summarises the findings and elaborates their implications for theory and practice.7

8.2 The Origins of Cross-Domain Deterrence

The shift in attention to CDD can be explained by two principal challenges. The first challenge relates to the progressive integration and synchronization of military operations across different domains (land, air, sea, cyber, and space) and the inherent disharmony between different levels of war (strategic, operational and tactical).8 This is because military organizations aspire to better integrate physical, social and communication technologies in their ability to apply violence in the pursuit of political objectives, leading to strategic compression and cross domain warfare. Multi-domain operations concepts are being developed to guide efforts to synchronise actions both horizontally across domains and vertically across levels of war.9 In light of the cross-domain nature of the challenge, strategists are envisaging analogous responses, including CDD.

The second challenge relates to the increased salience of “hybrid” or “grey zone” strategies that feature the simultaneous employment of military and non-military instruments, typically below the conventional military threshold, in an ambiguous fashion in order to evade attribution, with the goal to exploit adversary’s vulnerabilities, in the pursuit of political objectives.10 While the analytical value of the labels as such have caused considerable debate,11 the real-world impact of these strategies poses a serious strategic challenge. Their increased salience stems from the enormous costs associated with interstate wars, which makes major military powers disinclined from waging actual hot wars against each other. These powers therefore try and find alternative ways to achieve their political objectives—in line with the original tenets of the coercive diplomacy literature. Furthermore, the increased salience of grey zone strategies also derives from the opportunities offered by new avenues to hurt opponents due to technological and societal developments because of the global wiring of societies over the past quarter century. Strategically innovative actors have been making frequent use of these avenues over the past decade to considerable effect. These developments have led scholars and strategists to start thinking about the use and utility of cross domain deterrence in dealing with adversaries employing cross domain strategies also outside the traditional military domains.

Authors from both sides of the Atlantic generally concur that cross-domain deterrence involves the use of threats in one domain to deter activities in (an)other domain(s). Some authors define cross domain deterrence exclusively in the military domains land, sea, air, cyber and space albeit at different levels of abstraction. James Scouras, Edward Smyth and Thomas Mahnken assert for example that it is the prospect of retaliation from one domain to another which constitutes the essence of CDD.12 It is worth noting that the authors seem to focus exclusively on deterrence by punishment rather than denial. James Dawkins emphasizes that CDD involves the use of specific weapons rather than mere threats or retaliation in general. His conceptualization includes both punishment and denial strategies and draws attention to the actual instruments by which deterrent effects are to be achieved.13 Despite the differences in abstraction, these authors understand CDD to operate specifically within the military domains.

#### MDOs solve NATO Euro-Atlantic deterrence – BUT, organizational decentralization is key to efficacy

Lt. Gen. Andreas Marlow 21, German Army Lt. Col. Wilson C. Blythe Jr., U.S. Army, Lt. Gen. Andreas Marlow, German Army, is the commander of the NATO Rapid Deployment Headquarters, 1 German-Netherlands Corps. He has commanded at every level in the German Army. Marlow deployed as the Chief of Staff of the German contingent within NATO’s Kosovo Force mission, Deputy Chief of Staff-Operations Regional Command North International Security Assistance Force, and as the Chief of Staff Headquarters Resolute Support in Afghanistan. He is a graduate of the University of the Bundeswehr Hamburg, the German General Staff Officers Course, and the Command and Staff Course at the Canadian Forces College. Lt. Col. Wilson C. Blythe Jr., U.S. Army, is a strategist in the G-5 Plans of the 1 German-Netherlands Corps. He holds a bachelor’s degree in history from the University of Mississippi and a master’s degree in history from Eastern Michigan University. Blythe is a recipient of the Army Historical Foundation’s Distinguished Writing Award. His service includes deployments to Iraq and Afghanistan. 10-4-2021, "Multi-Domain Warfighting in NATO," <https://www.armyupress.army.mil/journals/military-review/online-exclusive/2022-ole/blythe/>, nihara, [brackets in original]

Since its formation in 1995 as a result of the merger of the Cold War-era 1 German Corps and 1 Dutch Corps, 1 German-Netherlands (GE/NL) Corps has repeatedly confirmed the commitment of its framework nations (Germany and Netherlands) to NATO, deploying to Afghanistan in 2003, 2009, and 2013. To continue this commitment, deter aggression, and defend the Euro-Atlantic area, 1 (GE/NL) Corps must demonstrate the ability to conduct large-scale combat operations as part of NATO against a peer enemy in an Article 5 scenario. The ability to conduct large-scale combat operations underpins the credibility of the Alliance’s deterrence and provides the basis for the defense of the Euro-Atlantic area in the event of conflict. This means that 1 (GE/NL) Corps must possess the ability to successfully perform the warfighting corps role, following its 2023 stand-by period as the NATO Response Force (NRF) Land Component Command (LCC).1

Execution of the warfighting corps role on the Euro-Atlantic multi-domain battlefields of today and tomorrow requires specific capabilities, in the required capacities, along with the expertise necessary to employ them in an Article 5 scenario against a peer enemy. As part of its transformation into a warfighting corps capable of multi-domain operations (MDO), 1 (GE/NL) Corps has conducted a campaign of learning consisting of academics, wargaming, and training and exercises. The results of this work are detailed below and specify the roles and responsibilities of a NATO warfighting corps within MDO, define the requirements and the structure for an MDO-capable warfighting corps, and describe the conduct of corps operations within the context of an Article 5 scenario.2

Organization

In contrast to stabilization operations in which the corps acted as a command-and-control node, for warfighting operations the corps functions not only as a headquarters but also as a formation that consists of its headquarters, combat and maneuver support forces, sustainment units, and other functional support units assigned to, attached to, or under the operational control of the corps.3 Also included are functional support capabilities operating in direct support of the corps or its subordinate divisions. Functional support units operating in the corps area of operations as general support, but not part of the corps, are normally not included in the corps formation.

When operating in the context of an Article 5 or warfighting operation, the corps is the highest tactical echelon. It is task organized for the operation, taking into account the operational and mission variables, and that task organization is dependent on the relative combat power of the enemy formations with which the corps will be engaged, the mission it receives, and the size of the area of operations in which it will operate. There are several proposed corps structures for the MDO battlefields of today and tomorrow. While there is much overlap to these proposals, the 1 (GE/NL) Corps structure was specifically developed to focus on the threats to the Euro-Atlantic area (see figure 1).4

Ideally, a NATO corps capable of conducting multi-domain operations within the Euro-Atlantic area includes the following:

2 to 5 divisions

1 x military intelligence brigade

1 x intelligence, surveillance, and reconnaissance (ISR) battalion equipped with unmanned aircraft systems (UAS) and unattended ground sensors (UGS)

1 x electronic warfare battalion

1 x corps fires command

2 x long-range artillery brigades

1 x cyber company

1 x ISR/targeting battery equipped with UASs and UGSs

1 x aviation brigade

1 x armored reconnaissance and surveillance brigade

1 x information warfare battalion

1 x psyops company

1 x engineer brigade (including chemical, biological, radiological, and nuclear [CBRN] capacity)

1 x air defence brigade

1 x signal brigade with a dedicated cyber defense organization

1 x rear area operations command

1 x sustainment brigade

1 x medical brigade

1 x military police brigade

1 x CBRN defense battalion

1 x civil affairs battalion with a political liaison team

1 x space battalion (includes high altitude companies for use as ISR or signal platforms)

Other forces may be assigned, attached, or provided operational control to give the corps additional capabilities) or additional capacity.5

**[FIGURE 1 OMITTED]**

Much of the structure above may sound familiar. However, based upon analysis conducted by 1 (GE/NL) Corps, this structure is better optimized to penetrate and dis-integrate the integrated air defense systems (IADS) and the integrated fires complex (IFC) that could challenge NATO forces in the Euro-Atlantic area. The presence of substantial long-range fires systems provides the corps with an organic capability to engage enemy fires systems and support assigned forces or other component commanders if conflict should occur. The corps’s capability to link a greater number of sensors than in the past, located throughout the depth of an expanded battlefield, to specific shooters enables it to converge capabilities in support of operational objectives and enhances the deterrent effect of Alliance ground forces.6

A key formation within the corps is the corps fires command, which integrates joint, interorganizational, and multinational targeting capabilities. The corps fires command plans, coordinates, and delivers joint all-domain fires to shape operations. The scale and scope of operations against a peer enemy generally necessitates multiple brigades of long-range rockets and missile systems. Two assigned field artillery brigades provide the corps with the means to defeat an enemy’s long-range and midrange fires and IADS to enable divisional tactical operations and freedom of maneuver for the Alliance joint force.7

Unlike a U.S. Army corps, a NATO corps does not fall under a standing theater army with organic capabilities or have subordinate divisions with a common and standardized divisional structure. Depending on the composition of the corps’s higher echelon and subordinate divisions and brigades, the corps may require additional capabilities or capacity. These capability gaps are most likely to be found in electronic warfare (EW), fires, ISR, and intelligence. During Article 5 operations, divisions will require additional assets to assist in converging effects from multiple domains. While the corps does not own space or special operations assets and its organic cyberspace capabilities are limited, it does possess the necessary tie-ins and expertise to integrate these domains into its operations. As the critical echelon in the execution of MDO, the corps will need the capacity to provide concurrent support to multiple divisions.8

Role of the Corps

1 (GE/NL) Corps is a multinational headquarters assigned to NATO. Therefore, NATO-compatible equipment (e.g., communication and information systems), and NATO processes and procedures (e.g., the operations planning process; data management platforms; and Allied Procedural Publication 28, Tactical Planning for Land Forces) will be used. It can translate operational inputs into tactical outputs. It synchronizes maneuver, fires, and effects with the requisite maneuver support and sustainment to shape the environment for subordinate forces to accomplish tactical missions and achieve operational and strategic objectives. This is accomplished through planning and mission orders to subordinate forces, making the best use of their capabilities and capacities while enforcing unity of command and achieving unity of effort.

To defeat the enemy, the corps executes five functions. It shapes the enemy forces in the corps deep area with available corps and joint capabilities;

maneuvers divisions and other combat formations to gain positions of advantage to close with and defeat enemy forces and compel their surrender or withdrawal, synchronizing the maneuver of divisions and, if necessary, brigades to reduce friction and coordinating the simultaneous maneuver of multiple formations in time and space;

initiates, executes, implements, ensures, and supports consolidation activities to set conditions for transition to a sustainable political end state;

sustains close, deep, and consolidation operations; and

generates combat power through RSOM&I and reconstitution.

The corps sets the conditions for subordinate divisions to focus on the close fight by integrating all elements of combat power in time and space to disrupt, interdict, and degrade the enemy while shaping the operating environment and enabling friendly forces to ensure freedom of action at the expense of its opponent. While the corps leverages Alliance joint capabilities to achieve effects in its area of operations, it is fundamentally a tactical and land-centric formation.9

In the conduct of its operations, it is essential that the corps sets an operational tempo that does not permit the enemy to recover and establishes an inexorable momentum using echeloned maneuver to ensure that once contact is gained, it is maintained. The corps feeds forces into the main battle area and controls the dispersion and mass of maneuver units. Divisions do the same at their level. The corps enables operational tempo at the division level by keeping enemy space, cyber, air defense, and long-range and midrange fires under constant pressure. This allows the divisions to finish decisively once they gain contact with the enemy. Momentum and tempo are vital and are metrics the corps commander uses to gauge success.10

Momentum and tempo are the threads that run through the corps’s operations and ensure that the enemy faces a continuous onslaught of simultaneous multi-echelon convergence. The importance of controlling the pace of operations challenges command and control because the corps must maintain forces not in contact to ensure fresh forces can reinforce success. The side that sets an overwhelming tempo will win. However, the speed component of tempo is not just speed of decision but also the cumulative speed of all our actions from planning and issuing orders to executing movements, fire missions, and transmitting decisions.11

Given the nature of the threats posed to the Euro-Atlantic area, an MDO-capable NATO corps must maintain joint, interservice, and multinational relationships to facilitate the quick transition to conflict. These relationships help prepare the corps for its role as the senior land tactical headquarters and are developed and maintained through multi- and bilateral training events and exchanges as well as the multinational layout of the headquarters itself. 1 (GE/NL) Corps emphasizes and trains the comprehensive approach in all phases of competition, conflict, and postconflict.12

The presence of a corps and its subordinate units serves as a deterrent force capable of simultaneously engaging multiple enemy combined arms armies and provides the means to shape the area of responsibility. During competition, the conduct of intelligence activities to set the conditions for successful combat operations will be a major focus of the corps. This work is essential to establishing the preconditions not only for a rapid transition to conflict but also for the achievement of tactical objectives. This includes the conduct of the threat systems analysis and comprehensive understanding of the operational environment (CUOE) necessary to support the convergence of Alliance, national, and organic assets necessary to achieve the desired effects against the enemy’s sophisticated and resilient layered standoff.13

The corps denies/deters the ability of an enemy’s ISR and EW systems to target NATO formations and facilities to gather information about capabilities. In addition, as deception is a key function of the corps, it will focus on deceiving and denying an adversary’s access to information related to current and future operating locations, units, and equipment.

To achieve decisive effects on an enemy during combat operations, the corps synchronizes and integrates combat power throughout the expanded battlefield. The ability of the corps to shape the lower operational and upper tactical environments is especially vital to Alliance operations during the initial period of a conflict when enemy long-range IADS will deny, or at a minimum contest, the Alliance’s use of the air domain. The contribution of the corps to the penetration and dis-integration of the enemy’s layered standoff is essential to generating freedom of maneuver for the Alliance joint force.14

During Article 5 or warfighting operations, the focus of the corps is on the conduct of the fight in the deep area with the objective of collapsing the enemy’s long-range and midrange IFC and IADS. The MDO-capable NATO corps utilizes an array of interconnected sensors—artillery delivered, UAS, cyberspace, space, and infiltrated—that place enemy systems at risk. These allow the corps to employ its long-range artillery to destroy targets throughout the depth of the corps area of operations. It is important to remember that this is not a targeting drill; these mid- and long-range enemy systems are attacked to enable maneuver and freedom of action. Only by defeating the enemy’s layered standoff will the Alliance be able to apply its air assets and will the corps’s subordinate divisions get to the close fight with the combat power to prevail.15

The corps is the central echelon in the planning and execution of MDO and is the lowest echelon capable of converging all domains. It creates the conditions for convergence at lower echelons by allocating resources, sequencing division maneuver, and incorporating it with deception. Especially within NATO, the corps will be the primary integrator and synchronizer of multi-domain capability in the forward conflict area and will array assigned capabilities to defeat enemy systems and enable tactical maneuver.

Much as it does with the air and maritime domains, the corps coordinates for—it does not execute—and integrates effects from the space and cyberspace domains through space and cyber support teams embedded in the command. These include effects to disrupt satellite communications to compound effects by organic EW against key command-and-control nodes to degrade enemy positioning, navigation, and timing, cyberspace and space-based ISR, and offensive cyberspace operations. Though the corps may not have the organic capabilities in all domains, it must possess the ability—to include the necessary staff bandwidth and expertise—to access effects from the space, cyberspace, and other domains.

By synchronising all reconnaissance and security operations across subordinate units, coordinating intelligence requirements, and fusing intelligence from multiple echelons, the corps supports echeloned maneuver and actively informs and integrates the full range of capabilities in all domains throughout the depth of the battlefield. Additionally, the corps unburdens subordinate formations by narrowing their focus, reducing their span of control, and maintaining the broader perspective in time and space, across the expanded battlefield. The planning horizon of a corps is typically seventy-two to ninety-six plus hours.16

While the corps’s focus is on the deep area, and much has evolved with MDO, the corps still supports division-level tactical maneuver. In the close fight, it will support its major subordinate units by reinforcing them with forces, especially in the main effort (Schwerpunkt) and by applying joint effects, fire support, air and missile defense, and to a limited extent, cyber defense. The corps will have to conduct information activities and additional stability tasks as well. The ability of the corps to provide this support to its subordinate divisions is especially critical in a multinational setting where the structure and capabilities of its subordinate divisions can greatly vary.17

To preserve the corps’s freedom of action for operations in the deep and close areas and to extend the force’s operational reach, in part through the generation or reconstitution of combat power, the corps must provide security in the rear area to prevent or minimize disruption of combat support and combat service support from the rear area forward and provide unimpeded movement of friendly forces throughout the rear area. To do this, the corps must be able to find, fix, and defeat enemy incursions into the rear area. This will require close coordination with host-nation defense and security forces, and nonmilitary actors.18

The corps must wage this fight to protect its formations in the rear and close areas while simultaneously waging a fight in the deep area to set conditions for exploitation, and it must manage forces out of contact to ensure exploitation can be sustained and reinforced. The corps must provide for the echelonment of formations to ensure depth and agility to maintain tempo once a penetration occurs.19

**[FIGURE 2 OMITTED]**

The corps protects its subordinate tactical formations from attacks originating in other domains. Especially important is the requirement to provide air and missile defense against the enemy’s substantial inventory of artillery and ground- and air-launched missiles. This will enable the divisions to engage in the close fight with favorable combat power ratios. To do this, the corps must not only possess the necessary air and missile defense assets but also incorporate deception and electromagnetic spectrum management into its operations. The main effort will be on proactive counterfire.20

To succeed, the corps must set the conditions prior to conflict (i.e., in competition). Especially important is the continuous conduct and refinement of the robust CUOE of the enemy required to understand its key systems so the corps can begin the penetration and dis-integration of the enemy’s mid- and long-range IADS and IFC during the transition to conflict. Vital to the success of these efforts is the corps’s ability to exercise command and control throughout the depth of the expanded battlefield. To command and control throughout the entirety of its area of operations, the corps will employ a distributive command post structure using multiple, dispersed, and mobile command posts.21

The corps area of operations and responsibility can extend up to 500 km deep and includes multiple echelons of tactical- and operational-level adversarial capabilities. Figure 2 illustrates how a corps operates across more than 60,000 km2 during large-scale combat operations. Assuming the corps consists of two divisions abreast, the area of operations for the corps could be 500 km x 120 km. In consequence, the corps area of influence would extend out 500 km/72 hrs., while the corps area of interest would extend out to 1,000 km/96 hrs.22 In this example, the corps rear area extends 200 to 250 km to the rear of the forward line of own troops.23

### centralization bad

#### Centralized implementation causes uninformed decisions – fails to control for accidents, biases, data poisoning AND weakness – turns the case AND causes unintended technological outcomes

Michael Horowitz & Kahn 20, Lauren Kahn, Michael C. Horowitz is professor of political science and the interim director of Perry World House at the University of Pennsylvania. Lauren Kahn is a research fellow at Perry World House at the University of Pennsylvania.1-14-2020, "The AI Literacy Gap Hobbling American Officialdom," War on the Rocks, <https://warontherocks.com/2020/01/the-ai-literacy-gap-hobbling-american-officialdom/>, nihara

Because AI is a general-purpose technology, the corresponding adoption challenges may prove especially difficult. There is a great deal of emphasis at present on how the United States can more effectively recruit and retain AI talent to work for the national security community and the government as a whole. This is critical, but the people making decisions about the use of algorithms from the situation room to the battlefield will not necessarily be informed about current developments in AI, let alone be AI experts, but military leaders and policymakers. Thus, a vital challenge is familiarizing and educating government leaders and policymakers about AI. This is a different challenge than that of incentivizing those with AI expertise to work for the U.S. government. Instead, it is about AI education for the policy community.

AI education for the policy community, from military leaders to Hill staffers to senior government officials, needs to happen now, as cases outside of the national security sphere illustrate. For example, in December 2017, the New York City council unanimously passed a bill that required the Office of the Mayor to form a task force dedicated to increasing transparency and oversight of the algorithms used by the city. A local city council member characterized the bill as essential, saying of the algorithms, “I don’t know what it is. I don’t know how it works. I don’t know what factors go into it. As we advance into the 21st century, we must ensure our government is not ‘black boxed.’”

This example touches on a key dynamic: Top policymakers — who are generally not technically trained — are at an increasing risk of being “black boxed” as technological complexity increases. This is especially true given questions even at the vanguard of AI research about the “explainability” of algorithms. However, organizational decisions about AI adoption and applications that “generally shape the impact of that technology” are being made today. Section 256 of the FY20 NDAA provides a first step towards national security literacy in AI, requiring the Secretary of Defense to develop an AI education strategy for military servicemembers. But there are questions about implementation, given well-known issues with professional military education, and the national security community more broadly requires AI literacy, not just military service members, since most policymakers are not in uniform.

The effective use of algorithms in the national security sphere requires basic education as well as recognition of what algorithms can and can’t do, the risks of automation bias and cognitive offloading to machines, the dangers of accidents and data poisoning, among other challenges. These need to be demystified and made relevant to national security officials, especially those senior leaders who may not consider themselves tech-savvy. It is impossible to hedge against potential dangers of a given technology if those using it do not fully understand and therefore many not be able to control it. Failure to control for biases, weaknesses, and accidents of even the most innocuous-seeming of algorithms has the potential to disrupt and create unintended policy outcomes that undermine US leadership in AI and US national security in general. Fortunately, there are a number of paths forward for effective AI education for end users, from online coursework to programs in civilian universities, to specially designed national security training programs.

#### AI policies made at high-levels causes erroneous deployment of technology – algorithmic influence on decision-making processes require clear understanding that senior policymakers don’t have

Michael Horowitz & Kahn 20, Lauren Kahn, Michael C. Horowitz is professor of political science and the interim director of Perry World House at the University of Pennsylvania. Lauren Kahn is a research fellow at Perry World House at the University of Pennsylvania, 1-14-2020, "The AI Literacy Gap Hobbling American Officialdom," War on the Rocks, <https://warontherocks.com/2020/01/the-ai-literacy-gap-hobbling-american-officialdom/>, nihara

Why and What?

In the years ahead, high level government leaders, despite having relatively rudimentary understanding of it, will make an array of formative decisions regarding AI, including funding, operations, assessing adversary developments, ethical and moral factors influencing adoption, managing associated employment issues, and so on. Adopting AI, from an organizational perspective, may therefore have several similarities to how entire organizations shifted in response to electricity, the combustion engine, the railroad, and other dramatic advances in prior centuries. AI is a wide-ranging technology that is already demonstrating the capacity to shape and alter the innumerable ways in which we engage with the world, from healthcare to soccer and everything in between.

Policymakers and national security officials will increasingly address AI-driven policies and technologies, make fundamental decisions based on machine learning techniques and algorithms, and help develop strong partnerships with those creating the technology. How do we ensure that decisions being made about AI at the top levels of government are well-informed ones, when policymakers, rather than technical experts, will make or review most of those decisions? And, practically speaking, what do they need to know?

Without baseline knowledge, policymakers won’t know what questions to ask, will be unable to frame what issues they are trying to solve as an “AI problem,” and might be overconfident in their understanding of AI and therefore what is feasible or practical. This could increase the chance of deployments of algorithms that lead to more errors and accidents than necessary. National security leaders need to be up-to-date on important innovations and factors that change global dynamics — such as AI has the potential to do. Being early adopters when it comes to functional knowledge for using algorithms is necessary so that leaders can conduct net assessments and subsequently make informed strategic decisions.

Beyond AI constituting an additional substantive dimension for consideration in planning and policy decisions, AI will also effectively change decision-making processes themselves. To the extent that some applications of AI, in the context of human-machine teams, may function as decision aids, those humans using the technology will need to have a level of understanding of how it works. To make optimal decisions about American AI policy and strategy, policymakers will need a clear understanding of AI principles and techniques — enough to understand how algorithms work and see potential benefits, but also recognize downside risks and avoid getting carried away by the hype.

#### Overcentralization will destroy military operations at the operational level

Rosario M. Simonetti 20, Lieutenant Colonel Rosario M. Simonett is an Italian Army Marine, “Automation and the Future of Command and Control The End of Auftragstaktik?,” Journal of Advanced Military Studies, Vol. 11 No. 1, June 2020, https://muse.jhu.edu/article/796245/pdf//RA

The impact of new technologies and the increased tempo of the future battlespace may overcentralize command and control functions at the political or strategic level. Political and strategic leaders might pursue preemptive or preventive wars as a strategy to acquire asymmetric advantage over the enemy, not because they must but because they can. As a result, senior leaders may be encouraged to bypass the advisory role played by their qualified staff and undermine the autonomy of lower level commanders. The advancement of technological systems may end mission command, Auftragstaktik. Donald E. Vandergriff defines Auftragstaktik as a cultural philosophy of military professionalism:

The overall commander’s intent is for the member to strive for professionalism, in return, the individual will be given latitude in the accomplishment of their given missions. Strenuous, but proven and defensible standards will be used to identify those few capable of serving in the profession of arms. Once an individual has been accepted into the profession, a special bond forms with their comrades, which enables team work and the solving of complex tasks. This kind of command culture . . . must be integrated into all education and training from the very beginning of basic training.

2 This article explores the roots of this trend, connecting historical perspectives with implications that next-generation technology may have on command and control.

Technological innovation plays a critical role in the conduct of war. The adoption of new technologies in warfare has been instrumental in replacing roles traditionally played by humans. During the interwar period, between World War I and World War II, warfare was optimized to cope with greater distances and faster execution through increasingly complex machines. The armed forces general staffs became more sophisticated and complex to process a greater amount of information. The battlefield gradually moved away from the commander, while command and control, a critical function for warfare, moved toward automation

Current military capabilities are the result of an evolutionary trend in which technology and information have constantly played a central role. With the introduction of the network-centric warfare (NCW) concept of operations, or the employment of networked forces at all levels, commanders can now access a network of sensors, decision makers, and soldiers, which provides shared awareness, higher tempo, greater lethality, and survivability on an almost global scale.3 The development and adoption of new technologies has allowed political and strategic decision makers to control the battlefield in real time even at the tactical level. The impact of new technologies and the increased speed in the future battlespace may overcentralize command and control functions at the political or strategic level. The consequences might be detrimental to the conduct of military operations at the operational and tactical level. In addition, autonomous weapons and artificial intelligence are the next step toward the automation of warfare with critical implications for command and control.

### airpower projection

#### Decentralization of AI implementation is key to airpower projection and flexibility – allows accurate data collection to perceive operational environments for effective execution

Matthew R. Voke 19, Major, USAF, 2019-11-01, “Artificial Intelligence for Command and Control of Air Power,” Air University Press, <https://apps.dtic.mil/sti/citations/AD1122447>, nihara

Decentralized Execution and Data

AI implementation may seem to imply a departure from decentralized execution because of the requirements for data and control. Decentralization of execution will remain an essential tenet of airpower. Decentralized execution is a requirement because of uncertainty, friction, changes, communication limitations, and ambiguity. Decentralization allows aircrew to seize the initiative, be responsive to uncertain and changing environments, and fosters flexibility in lower-level commanders. The most significant immediate change in airpower execution because of AI implementation is the requirement for increased data collection. As previously discussed, data is a fundamental requirement of AI learning and performance. AI cannot accurately perceive the environment and make decisions without sufficient data collection. Future leadership will likely highlight data collection and timely reporting requirements throughout levels of air operations to ensure the feedback loop is robust. Commanders must clearly express intent to operators and assist their decentralized execution, giving them the proper tools and situational awareness to execute upon intent. Operators owe timely and accurate truth data and reliably accurate execution to their commanders in return for delegated execution authority.

#### Decentralization’s key to airpower agility – otherwise tension between political control and military execution causes data gaps AND inefficiencies that complicate operational implementation

---AOC = air operations center, the senior element of the theater air control system

Matthew R. Voke 19, Major, USAF, 2019-11-01, “Artificial Intelligence for Command and Control of Air Power,” Air University Press, <https://apps.dtic.mil/sti/citations/AD1122447>, nihara

Centralization Versus Decentralized Airpower

US doctrine prescribes the conduct of joint air operations using the principle of centralized control and decentralized execution.22 An oversimplified synopsis driving this tenet of airpower is that centralization of control enables the senior echelon commanders to control, mass, and lead forces effectively; decentralization of execution allows forces to seize the initiative, respond to uncertain and changing environments, and fosters flexibility in lower echelons.

Technological developments frequently shift the equilibrium of this tenet of airpower. Robust communications connectivity has increased the shared operations picture at all levels, but it has also enabled senior leadership involvement in the finest details of employment.23 This duality has created inherent tension between the imperatives of political control and those of efficient mission accomplishment that leaders must understand.24 Although centralized control and execution are possible in many situations, a conscious effort to delegate execution authority appropriately will ensure the maintenance of US airpower agility.

The balance of centralization and decentralization can shift between and during conflicts, and leaders must strive to increase what some call “agility” in airpower employment. The Air Force Future Operating Concept defines agility as the ability to react rapidly to situations. Agility is a combination of one’s flexibility, speed, coordination, balance, and strength.25 Decentralization generally favors flexibility and speed, while centralization generally favors coordination and strength. One’s understanding of agility might imply physical capability, but agility also includes a cognitive capability to react to a dynamic opponent, moving target, or shifting environment.26 The power of AI employment in airpower C2 lies in the cognitive speed and strength it can bring synergistically toward the goal of agility.

C2 Structure

C2 systems control joint air operations, typically built around the C2 system of the service component commander, that has the preponderance of air assets and the most exceptional ability to control them.27 The air operations center (AOC) is the senior element of the theater air control system, which ensures the effective planning and conduct of air, space, and cyberspace operations. The AOC construct may also apply when fighting with joint or coalition partners as a joint air operations center or a coalition air operations center. The size of an AOC can vary wildly between staff in the single digits to more than a thousand officers, enlisted, and civilian members. Each AOC’s organization differs, but their common goal is to match available means toward tasked military objectives. The responsibilities of the AOC typically include planning and controlling joint air operations, recommending priorities in air apportionment, airspace coordination, air defense coordination, space coordination, and cyberspace coordination.

Technological improvements in computing, communications, and information sharing have disrupted the tiered C2 structure creating disruptions from operational planning to tactical execution. AOC leadership is capable of making decisions historically conducted at lower operational or tactical echelons. Today, for example, the highest levels of operational C2 may not delegate target identification and weapons release authority, which was once only possible at the tactical edge. The relative overmatch wielded when facing less capable adversaries, and the aversion to civilian casualties and loss of life may have lulled the United States into complacency and a false assumption that future wars will take place in the same benign environments.28 Increases in efficiency and agility needed to defeat near-peer adversaries are possible through distributing control outside the AOC, decentralizing the execution of air assets, and leveraging AI’s speed and cognitive strength across multiple levels of C2.

The C2 of airpower has excellent potential to leverage AI augmentation and automation for increased cognitive agility. The next section discusses one example of AI use area in airpower C2—joint targeting. There are currently data gaps and inefficiencies within the targeting cycle that complicate the efficient transfer of critical information when planning and executing joint air operations.29 The next sections will cover how AI can prepare decision-makers with a better understanding of their operating environment, filter and fuse the fire hose of battlefield data into relevant information, and increase decision speeds.

#### Specifically, NATO airpower projection combined with forward presence deters Russian aggression in the Baltics – otherwise fractures EU and NATO which collapses the LIO

Major Morgan P. Lohse 16, Maj Morgan Lohse received his commission through Officer Training School at Maxwell Air Force Base, AL in 2003. He earned his aeronautical rating as a navigator at Naval Air Station Pensacola, and has since served in operational and formal training assignments. Prior to attending the School of Advanced Air and Space Studies, he attended Air Command and Staff College at Maxwell Air Force Base. US Air Force, June 2016, “From Power Projection to Power Protection: Revitalizing Conventional Deterrence in NATO,” School of Advanced Air and Space Studies Air University Maxwell Air Force Base, Alabama, <https://apps.dtic.mil/sti/pdfs/AD1030417.pdf>, nihara

Power Strategies

The emergence of global US interests led the United States to diversify its approach to the use of military force. Until World War II, the United States did not maintain large standing military forces in peacetime. Instead, the pre-Cold War model relied on a build-up and mobilization of forces, which then deployed to distant lands such as the Philippines or Western Europe when crises loomed. The Berlin Crisis in 1948 and further Communist antagonism ushered in a new model of large peacetime military forces coupled with forward basing. These bases enabled the protection of allies that were still broken from World War II and served as a deterrent to Soviet aggression.

The initial NATO Cold War strategy relied on large conventional forces stationed at forward bases to deter and defend against massive Soviet armored formations. As the costs of these large standing forces increased, NATO adopted a deterrence strategy that relied heavily on nuclear weapons, which ameliorated NATO’s acknowledged conventional inferiority. Over time, questions arose about the credibility of this nuclear deterrent, and a conventional focus to NATO’s force posture returned. This conventional focus merged elements of projecting power from the United States and Western Europe to Central Europe in an expeditionary approach with protecting allies through forward presence that provided a front line and a trip-wire until reserves could arrive.

The end of the Cold War resulted in drastic changes in the global US force posture. The lack of a competitor led to the withdrawal of tens of thousands of military personnel stationed overseas at major operating bases. The emergence of terrorist threats enhanced this dynamic as the US military shifted its focus to counter-terrorism and counterinsurgency operations in Southwest Asia and the Middle East. The post-9/11 world facilitated a force posture approach that relied on generation of military forces in the United States; these forces rotated abroad for deployments ranging from three to fifteen months. This model of power projection proved stressing in its own right but was a solution to a complex problem that largely precluded the permanent basing of US forces in the Middle East and Southeast Asia.

The return of great power competition finds the US military with a force posture that reflects the needs of limited interventions and counterinsurgency. The US military has adapted this model to great power competition through the rotation of forces to deter and show resolve in both Europe and the Pacific. The drawback of this approach is that it lacks demonstrable commitment and credibility against a peer competitor, especially in that competitor’s backyard.

A Balanced Approach

An appropriate strategy for NATO requires permanent forward presence. NATO is in a new era of great power competition within a context of general deterrence. Russia has not specifically threatened the Baltic states or other Eastern European NATO member states, but its foreign policy and military modernization demonstrate that it is reasserting itself on the world stage. Russia’s anti-access capabilities complicate the matter, through air and ground based systems that could prevent NATO from delivering additional forces into Eastern Europe. For the Baltics, general deterrence of Russia requires credible military force on a permanent basis. Permanent forward basing of any force is costly financially and politically, but permanently stationed ground forces demonstrate greater commitment, and additional airpower will help mitigate Russia’s anti-access capabilities.

To revitalize the deterrent credibility of NATO vis-à-vis Russia, NATO must increase its protection of member states through forward presence rather than relying on power projection from expeditionary or rapid response forces. NATO should take a balanced approach that combines elements of the power projection, expeditionary model with a protective, forward presence model. Only a balanced strategy that includes forward presence will provide an enduring deterrent to Russian aggression at NATO’s borders.

Significant increases in forward basing of military personnel and equipment will test the political resolve of NATO and the United States. Politicians must determine the utility of NATO in terms of both the security it offers and its potential as a binding organization of the liberal order. What would happen to NATO if Russia invades a member nation? Would NATO be able to defend or liberate that nation utilizing its current power projection strategy? The Baltics are also European Union (EU) members, and fracturing the EU could have its own implications for the liberal order. In comparison to the political cost of failure, the cost of fielding an increased, permanent forward presence is small. Only with political will, however, can NATO adjust to an era of renewed competition.

Overview

There are two conventional strategies for deterrence, power projection and power protection. Power projection evolved during the Cold War to the prominent place it holds in current national military strategy. Airpower is critical to power projection. Without air superiority, power projection is ineffective. On the other hand, forward presence is the safest strategy to deter an aggressor from seeking a rapid military victory, but it also requires more resources. Most importantly, the strategies of power projection and power protection require tailoring to the specific security context rather than rote application of the traditional strategy.

The following analysis includes the Cold War and post-Cold War evolution of US military force posture, and Russia’s return as a great power to include Russian anti-access capabilities. The deterrence focus is in terms of territorial acquisition as opposed to other objects of deterrence such as use of weapons of mass destruction, terrorism, or other actions. Examination is within the framework of general deterrence and the strategy behind force postures, to include the evolution, execution, and suitability of these strategies to today’s current power competition. Limitations of this short work include a focus restricted to general deterrence rather than on other elements of coercion, and a focus on how force postures generate deterrence, instead of other factors such as doctrine, readiness, and weapons technology.

Chapter 1 analyzes conventional deterrence within the larger structure of strategic coercion and focuses the scope of this thesis on general deterrence and the prevention of a fait accompli or rapid military victory. It includes analysis of two distinct deterrent strategies, power projection and power protection, but also highlights the limitations of any deterrent policy and warns of the consequences of deterrent failure.

Chapter 2 explains the evolution of NATO’s force posture during the Cold War, tracing the rise of power projection strategies utilizing expeditionary forces from US bases, and highlights the importance of airpower to such a strategy. Chapter 3 analyzes the change to an almost exclusive reliance on power projection after the Cold War as US attention shifted from great power competition to a variety of security threats, and underscores the importance of diplomacy, strategic warning, and airpower.

Chapter 4 describes the challenges of adapting the power projection strategy to great power competition in an anti-access, areadenial (A2AD) environment, and investigates the evolution of the current deterrent strategy. This chapter recommends a NATO strategy that balances power projection with increased protective forward presence. Finally, the conclusion underscores key recommendations, and frames other security challenges within an appropriate category of strategic coercion to provide a foundation for further analysis. Russia’s annexation of Crimea and continuing actions in Ukraine demonstrate that NATO’s Eastern European countries require stronger deterrence. A quick Russian military victory in a Baltic state would be difficult to reverse and could fragment NATO and the European Union. While power projection has served the United States well since the end of the Cold War, deterrence in Europe requires protective forward presence.

### ---lio !

#### Extinction---rogue tech, bio arms-racing, and climate change

Harari ’18 [Yuval; September 26; Professor of History at Hebrew University of Jerusalem; "We need a post-liberal order now," https://www.economist.com/open-future/2018/09/26/we-need-a-post-liberal-order-now]

Even more importantly, whether people like it or not, humankind today faces three common problems that make a mockery of all national borders, and that can only be solved through global cooperation. These are nuclear war, climate change and technological disruption. You cannot build a wall against nuclear winter or against global warming, and no nation can regulate artificial intelligence (AI) or bioengineering single-handedly. It won’t be enough if only the European Union forbids producing killer robots or only America bans genetically-engineering human babies. Due to the immense potential of such disruptive technologies, if even one country decides to pursue these high-risk high-gain paths, other countries will be forced to follow its dangerous lead for fear of being left behind.

An AI arms race or a biotechnological arms race almost guarantees the worst outcome. Whoever wins the arms race, the loser will likely be humanity itself. For in an arms race, all regulations will collapse. Consider, for example, conducting genetic-engineering experiments on human babies. Every country will say: “We don’t want to conduct such experiments—we are the good guys. But how do we know our rivals are not doing it? We cannot afford to remain behind. So we must do it before them.”

Similarly, consider developing autonomous-weapon systems, that can decide for themselves whether to shoot and kill people. Again, every country will say: “This is a very dangerous technology, and it should be regulated carefully. But we don’t trust our rivals to regulate it, so we must develop it first”.

The only thing that can prevent such destructive arms races is greater trust between countries. This is not an impossible mission. If today the Germans promise the French: “Trust us, we aren’t developing killer robots in a secret laboratory under the Bavarian Alps,” the French are likely to believe the Germans, despite the terrible history of these two countries. We need to build such trust globally. We need to reach a point when Americans and Chinese can trust one another like the French and Germans.

Similarly, we need to create a global safety-net to protect humans against the economic shocks that AI is likely to cause. Automation will create immense new wealth in high-tech hubs such as Silicon Valley, while the worst effects will be felt in developing countries whose economies depend on cheap manual labor. There will be more jobs to software engineers in California, but fewer jobs to Mexican factory workers and truck drivers. We now have a global economy, but politics is still very national. Unless we find solutions on a global level to the disruptions caused by AI, entire countries might collapse, and the resulting chaos, violence and waves of immigration will destabilise the entire world.

This is the proper perspective to look at recent developments such as Brexit. In itself, Brexit isn’t necessarily a bad idea. But is this what Britain and the EU should be dealing with right now? How does Brexit help prevent nuclear war? How does Brexit help prevent climate change? How does Brexit help regulate artificial intelligence and bioengineering? Instead of helping, Brexit makes it harder to solve all of these problems. Every minute that Britain and the EU spend on Brexit is one less minute they spend on preventing climate change and on regulating AI.

In order to survive and flourish in the 21st century, humankind needs effective global cooperation, and so far the only viable blueprint for such cooperation is offered by liberalism. Nevertheless, governments all over the world are undermining the foundations of the liberal order, and the world is turning into a network of fortresses. The first to feel the impact are the weakest members of humanity, who find themselves without any fortress willing to protect them: refugees, illegal migrants, persecuted minorities. But if the walls keep rising, eventually the whole of humankind will feel the squeeze.

### ---eu !

#### EU strength prevent global conflict and transnational threats – extinction

--stolen from the EU CP file ☺

Dr. Rosa Balfour 19, Senior Transatlantic Fellow at the German Marshall Fund of the United States, PhD in International Relations from the London School of Economics and Political Science, MA in History from Cambridge University, MSc in European Studies from the London School of Economics and Political Science, Senior Advisor to the European Policy Centre, Associate of LSE Ideas, “The European Foreign Policy in a Hostile Environment”, The Progressive Post, 4/11/2019, https://progressivepost.eu/debates/next-economy/european-foreign-policy-hostile-environment

In a brittle world without enduring strong international alliances, the debate on Europe’s ‘strategic autonomy’ has gained new resonance, but it should not shadow the EU’s unique key international assets in the global economy and multilateral order. Working with global networks to promote norms and public goods is key to push back on nationalism, the rise of geopolitics and transactionalism.

Strategic autonomy’ and ‘complementarity with NATO’ usually appear in the same sentence in the European debate – the latest doctrinal iteration to be found in the EU Global Strategy of June 2016. The ensemble reflects Europe’s need to rely on its transatlantic relationship for security and territorial defence, empowering it to carry out foreign policy too. The EU’s greatest foreign policy achievement of enlarging to Central Europe after the Cold War, pursued in tandem with NATO expansion, is testimony to this pairing.

Since the end of 2016, the US President’s international preferences undermine directly or indirectly Europe’s security. Whether it is the insistence on greater burden-sharing, US action in the Middle East, or trade disputes with China, current US policies put Europe’s security – already challenged by Russian action in Eastern Europe and the Middle East – at risk.

European leaders have started to question whether the transatlantic relationship needs to be preserved no matter what, or whether Europe should emancipate from it. The debate on ‘strategic autonomy’ is animating recent efforts in the field of security and defence. It refers to the ability to make and carry out decisions on defence, to conduct military operations autonomously, and to have the industrial capabilities to do so. Even if this level of strategic autonomy were agreed upon, it would take a generation for Europe to affect the world stage.

The focus on strategic autonomy speaks to present insecurities in European societies, but not to the EU’s international legitimacy where, possibly, the European Union has better opportunities to develop means of political autonomy which befit its history and international identity. The emerging debate on economic sovereignty is addressing for the first time the degree to which the EU can make political use of some of its economic and financial tools, such as the Euro as an international currency. After all, the EU and its Member States remain the world’s largest trade bloc and donor.

On the multilateral stage, Europe faces an increasingly hostile environment but remains the best hope to pursue universal principles, such as human rights and the rule of law, which underpin the resilience of that multilateral system. How to partner with other countries and actors around the globe to push back on attacks to international order is no longer a second order priority.

If the way ahead appears clear, achieving it is a tall order. The rationale for collective action for the EU seems obvious – the ‘politics of scale’, or to be stronger together rather than weaker apart – but historically difficult to achieve. The multiple threats and risks on Europe’s doorsteps have only minimally bridged the strategic divergence that continues to beset the continent, and the rise of the populist radical right is beginning to undermine existing European external policies, not to speak of a higher level of ambition.

Looking at global politics from a non-European perspective, how Europe’s friends and partners around the world will welcome a bid for greater autonomy – politically, economically, and strategically – still needs to be seen. The EU’s worldview that it has acted as a ‘force for good’ is not uncritically accepted. After all, that ethical stand was also possible thanks to the EU’s belonging to a stable and hegemonic West.

If Europe wants to engage with the world and simultaneously strengthen its strategic identity it needs to square some circles. Without giving into the facile critique that realism and geopolitics render multilateral principles obsolete and warrant hard-nosed politics, Europe should leverage its assets, which are irrevocably embedded in multilateralism and cooperation. Climate change, conflict prevention and mediation, and an open and fairer international trade system are among the assets that the EU can concretely work towards globally.

To do so it needs to engage flexibly with global actors, focusing more on multilevel networks including civil society rather than on the traditional partnerships between governments, some of which are no longer benign or useful. Both will require a dose of humility in listening to non-European world views and of pragmatism in seeking appropriate strategies and paths forward.

Last but not least, if Europe wants to imagine its own history of prosperity, democracy and peace as still relevant to the debates taking place in the rest of the world, it also needs to think about the global future sustainability of welfare, taking progressive politics outside national boundaries and engaging in a more global and open debate about public common goods.

## Case Answers

### 1nc – pilot projects fail

#### Pilot projects lack reliable information on durability, monitoring, and cost – no scale up

--title of card is specific to digital health system integration

--BUT, this section of the card is applicable to pilot projects broadly – all the warrants for why pilot projects are bad are reasons that would apply to the plan i.e. there’s no monitoring once deployed limiting the impact of investment, there’s no longevity so we can’t assess durability of cost due to short-term nature and it doesn’t represent data or provide enough information

Alain Labrique et al 18, “Establishing Standards to Evaluate the Impact of Integrating Digital Health into Health Systems.” Global health, science and practice vol. 6,Suppl 1 S5-S17. 10 Oct. 2018, doi:10.9745/GHSP-D-18-00230, nihara

Inadequate focus on monitoring the quality of programs, once deployed, has led a number of large digital investments to have limited impact.50 Just as with non-digital projects, research and guidance on fidelity and quality must be part of implementation planning for long-term stability. Resources and improved tools must be developed to facilitate program monitoring—from system functionality to staff performance quality. Few projects, globally, have reached a level of scale or longevity needed to provide insight into the actual anticipated and unanticipated costs of large digital health operations. In contrast to many decades of well-documented operational costs for paper-based systems, program planners lack reliable information on the durability of digital assets, necessary overages, and contingency procurements to allow for digital device failures or losses. Models estimating the total cost of ownership or operational costs are often based on short-term programs or extrapolated from pilot and research environments, which may not accurately represent real-world data. Economies of scale and cost-savings possible through the use of shared digital assets remain underexplored. Finally, understanding the collateral gains to be made from digital investments can also strengthen the case for these investments; that is, the time and effort previously spent on manual data summarization or aggregation—often repeated at multiple health-system levels—can be liberated for repurposing to other primary-care tasks.

### 1nc – testing fails

#### DoD can’t operationalize AI at scale

Danielle C. Tarraf 21, William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, Ali Wyne, Daniel Elinoff, Edward Geist, Benjamin N. Harris, Eric Hui, Cedric Kenney, Sydne Newberry, Chandler Sachs, Peter Schirmer, Danielle Schlang, Victoria M. Smith, Abbie Tingstad, Padmaja Vedula, and Kristin Warren, The Department of Defense's Posture for Artificial Intelligence: Assessment and Recommendations for Improvement. Santa Monica, CA: RAND Corporation, 2021. <https://www.rand.org/pubs/research_briefs/RB10145.html>, nihara

Once again, artificial intelligence (AI) is at the forefront of our collective imaginations, offering promises of what it can do to solve our most challenging problems. As the news headlines suggest, the U.S. Department of Defense (DoD) is no exception when it comes to falling under the AI spell. But is DoD ready to leverage AI technologies and take advantage of the potential associated with them, or does it need to take major steps to position itself to use those technologies effectively and safely and scale up their use? This is a question that Congress, in its 2019 National Defense Authorization Act (NDAA), and the Director of DoD's Joint Artificial Intelligence Center (JAIC) asked RAND Corporation researchers to help them answer. This research brief summarizes that report.

Artificial Intelligence and DoD

The term artificial intelligence was first coined in 1956 at a conference at Dartmouth College that showcased a program designed to mimic human thinking skills.[1] Almost instantaneously, the Defense Advanced Research Projects Agency (DARPA) (then known as the Advanced Research Projects Agency [ARPA]), the research arm of the military, initiated several lines of research aimed at applying AI principles to defense challenges (see Figure 1). Since the 1950s, AI — and its subdiscipline, machine learning (ML)[2] — has come to mean many different things to different people: For example, the 2019 NDAA cited as many as five definitions of AI, and no consensus emerged on a common definition from the dozens of interviews conducted by the RAND team for its report to Congress.

To remain as flexible as possible, the RAND study was not bound by precise definitions, asking instead, "How well is DoD positioned to build or acquire, test, transition, and sustain — at scale — a set of technologies broadly falling under the AI umbrella"? And if those technologies fall short, what would DoD need to do to get there?

**[FIGURE 1 OMITTED]**

The RAND team distilled the NDAA's mandate into the following three guiding questions:

What is the state of AI relevant to DoD?

What is DoD's current posture in AI?

What internal actions, external engagements, and potential legislative or regulatory actions might enhance DoD's posture in AI?

For the first question, the RAND team purposely avoided trying to determine what technologies DoD should pursue or how DoD currently measures up to other countries in terms of AI uptake because that was outside their mandate. Rather, the team assessed what DoD decisionmakers need to know about AI.

For the second question, the team assessed the posture of DoD for AI using a framework of six dimensions (Table 1).

Table 1. DoD's Posture for AI Was Assessed Across Six Dimensions

Dimension Components

Organization Vision, strategy, and resource commitments

Organizational structures

Stakeholders and their mandates, authorities, and roles

Advancement Research and development portfolio and activities

Prototyping

VVT&E

Adoption Procurement

Fielding, sustainment, and life-cycle management

Development of doctrine; concepts of operations; tactics, techniques, and procedures; and processes

Innovation Internal culture of innovation

Mechanisms for leveraging external innovations

Mechanisms for engaging external innovators

Data Data as a resource

Governance of data collection and use

Storage, computing, and other infrastructure

Tal-ent Talent needed to develop, acquire, sustain, and operate

Recruitment, retention, cultivation, and growth

Career management

What Are the Recent Leap-Ahead Advances in AI and ML?

Deep learning, a form of supervised machine learning, trains many-layered neural networks on large sets of labeled training data to accomplish classification and prediction tasks, thereby offering new solutions to long-standing image, text, and speech-recognition problems.

Deep reinforcement learning uses deep learning to solve for approximate solutions of sequential decisionmaking problems with deferred rewards and has applications in strategic and computer games.

What Decisionmakers Need to Know About AI

Examining the implications of AI for DoD and strategic decisionmaking requires taking a holistic view that considers three critical elements and how they interact:

* the technology and capabilities space
* the spectrum of DoD AI applications
* the investment space and time horizon.

The technologies and capabilities space: This includes the approaches, such as algorithms, that underpin current AI solutions. Although many technologies underpin AI, current interest (and hype) is fueled by advances in a small number of areas, like deep learning.

But success in deep learning requires large data sets. Deep learning algorithms tend to be highly specific to the applications for which they were designed, and demonstrated applications have tended to be commercial. What's more, VVT&E remains very challenging across the board for all AI applications, including safety-critical military applications.

**[FIGURE 2 OMITTED]**

The spectrum of DoD applications: The spectrum of DoD AI applications can be characterized by where those applications fall in terms of four independent factors: operating environment, resources, tempo, and implications of failure (see Figure 2). The position on this spectrum can be summarized in terms of three overlapping bins:

* enterprise AI, consisting of such applications as the management of health records at military hospitals in well-controlled, slower-paced environments, where analysts and decisionmakers have access to ample computational resources, data might be considered recoverable, and implications of failure might be negligible
* mission-support AI, consisting of applications like the Algorithmic Warfare Cross-Functional Team, also known as Project Maven, which aims to use ML to assist humans in analyzing large quantities of imagery from full-motion video data collected in the battle theater by drones
* operational AI, consisting of applications of AI integrated into weapon systems that must contend with dynamic, adversarial environments; fast tempo; scarce computational and communication resources (and possibly data); and significant implications of failure for casualties and risks to strategic objectives.

The investment space and time horizon: In addition to the investments needed to develop or acquire AI technologies across the spectrum of applications, success in AI requires the following three other kinds of investments:

* technological and other enablers, such as infrastructure to enable the collection and management of data
* VVT&E foundations and practice for technological checks and balances
* foundational basic research that is not specifically aligned with a particular product or application to maintain longer-term technological superiority.

Finally, to manage expectations and ensure continued support, it is important to set realistic goals for the lead times that AI will need to progress from demonstrations of what is possible to full-scale implementations in the field. The RAND team's analysis suggests that, as a rule of thumb, sustained DoD investments made as of the time of the original report's publication (2019) can be expected to yield at-scale deployments in the

* near term (up to five years) for enterprise AI
* middle term (five to ten years) for most mission-support AI
* far term (longer than ten years) for most operational AI applications.

Of course, DoD can expect and should pursue faster progress for some applications, even within operational AI. However, these timelines reflect the RAND team's assessment of what reasonable expectations are, given the current state of the technology and taking into account the four factors discussed previously: operating environment, resources, tempo, and implications of failure.

DoD's Posture for AI

Overall, the RAND team found that, despite some positive signs, DoD's posture is significantly challenged across all dimensions of the posture assessment.

Organizationally, at the DoD level, the current DoD AI strategy lacks both baselines and metrics for assessing progress. Thus far, the JAIC has not been given the authority, resources, and visibility needed to scale AI and its impact DoD-wide. Similar challenges are seen at the level of the individual services.

Data are often lacking, and when they exist, they often lack traceability, understandability, accessibility, and interoperability.

The current state of VVT&E for AI technologies cannot ensure the performance and safety of AI systems, especially those that are safety-critical.

DoD lacks clear mechanisms for growing, tracking, and cultivating AI talent, a challenge that is only going to grow with the increasingly tight competition with academia, the commercial world, and other kinds of workspaces for individuals with the needed skills and training.

Communications channels among the builders and users of AI within DoD are sparse.

Current DoD practices and processes — or their implementation — might be hampering innovation within DoD and inhibiting DoD's ability to bring in external innovation.

Despite some positive signs, DoD is poorly positioned across all dimensions to effectively leverage and scale AI. The report offered a set of recommendations, both strategic and tactical, for moving forward.

#### Our studies are comprehensive assessments of DoD capability that indicate structural issues in that inhibit AI

Danielle C. Tarraf 19, William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, Ali Wyne, Daniel Elinoff, Edward Geist, Benjamin N. Harris, Eric Hui, Cedric Kenney, Sydne Newberry, Chandler Sachs, Peter Schirmer, Danielle Schlang, Victoria M. Smith, Abbie Tingstad, Padmaja Vedula, and Kristin Warren, The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations. Santa Monica, CA: RAND Corporation, 2019. <https://www.rand.org/pubs/research_reports/RR4229.html>, nihara

Approach

The starting point of our study was the underlying premise, implicit in the language of Section 238 of the FY 2019 NDAA, that DoD needs to be competitively positioned for AI. Motivated in part by the desire to remain agnostic about the precise definition of AI, we posed the question: How well is DoD positioned to build or acquire, test, transition, and sustain—at scale—a set of technologies falling under the broad AI umbrella?

We distilled the information needed to answer that question into six dimensions that form the analytical framework for our posture assessment. These are organization (executive-level view of DoD, including vision, strategy, organizational structures, and resources committed); advancement (research, development, prototyping, and verification, validation, testing, and evaluation of the technology); adoption (technology procurement, fielding, and life-cycle management and redesign of concepts and processes to make best use of the technologies); innovation (internal culture for innovation and mechanisms for bringing in external innovations or innovators); data (data as a resource, data governance, and supporting infrastructure allowing the leveraging of data); and talent (DoD needs and mechanisms for cultivating and growing talent).

We initiated four parallel data collection and analysis efforts. The first line of effort collected input from 59 DoD interviews and nine other federal government interviews relating to all six dimensions of posture assessment to help us better understand the current DoD and federal landscape. The second line of effort collected input from 25 industry interviews and nine academic interviews relating to all six dimensions of posture assessment to help us better understand best practices and lessons learned. The third line of effort developed six historical case studies to help us understand lessons learned from history that might be extrapolated to the current posture assessment. The data and insights from these three lines of effort were synthesized and supplemented by two additional sources: first, the team’s technical and other expertise, and second, our consultation of the literature. Emerging themes and evidence across these multiple sources were then used as the basis for our assessments of the state of AI and DoD’s posture in AI, and to develop a set of recommendations.1 The fourth effort was a quantitative assessment of DoD’s current investment portfolio in AI; that effort is discussed in an annex to this report that is not publicly available.

### 1nc – no operationalization

#### No operationalization – lack of military integration with scientific and technological thresholds cause pilot projects to fail

--OE: operational environments

Courtney Crosby 20, Courtney Crosby, PhD, is the chief scientist with Booz Allen Hamilton’s Strategic Innovation Group. She has a PhD in decision sciences, with a focus on battlefield artificial intelligence (AI) systems for the Department of Defense. Crosby has deployed several times in support of various overseas missions. In her current role, she spearheads AI operationalization and innovation within the military C5ISR domain. Her previous experience includes research and development of emerging capabilities and social science analysis relevant to human machine teaming, 2-5-2020, "Operationalizing Artificial Intelligence for Algorithmic Warfare," Military Review, Army University Press, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2020/Crosby-Operationalizing-AI/>, nihara

Conflict can be won or lost based on military offsets, or means with which defense units can asymmetrically combat adversarial advantages. With great-power competition, adversarial technology overmatch, and ever-expanding theaters, conventional offsets are often augmented by artificial intelligence (AI).1 Yet, the Department of Defense’s (DOD) ability to operationalize AI is nascent.2 Initial AI programs adopted by the Pentagon focus on the transfer of commercial capabilities to the defense sector, thus highlighting technical performance and deemphasizing mission-oriented function.3 As a result, initial pilot projects have failed to move into real-world operational environments (OE).

Operationalizing Artificial Intelligence

Operationalization hinges on the understanding that AI is not an end state but rather one way of achieving a military advantage. To that end, the technical execution of AI-related methodologies must be married to the OE. This consideration diverges from traditional thought because AI solutions are typically developed to achieve a certain statistical threshold (e.g., recall, precision), rather than a military objective (e.g., increased standoff distance).4

This dynamic is confounded by the term “algorithmic warfare,” which currently conflates technical and military characterizations. Algorithmic warfare intends to reduce the number of warfighters in harm’s way, increase decision speed in time-critical operations, and operate when and where humans are unable to operate.5 Yet, none of those objectives speak to mathematics or computer science; they are grounded squarely in military end states. The problem is that the bridge between science, technology, engineering, and mathematics disciplines and military end states was never established before the Pentagon embarked on its AI trajectory.

The desired bridge is a framework for guiding and assessing AI operationalization, with algorithm performance on one side and mission utility on the other. Such a combination ensures that mathematical equations can prove or numerically validate an AI system while qualitative benchmarks guarantee practical application. The result is algorithmic warfare based not just on statistics but a broader architecture for operational relevancy. That relevancy is couched in five requirements:

* minimum viability,
* the ability to adapt to unknown and unknowable scenarios,
* the prioritization of insight over information,
* the requisite level of autonomy for the application, and
* battlefield readiness.

For the first time, such requirements lay the foundation for assessing military AI programs and defining success.

### 2nc – dod fails – data / talent

#### DoD fails –

#### data:

#### 1 – BOTH storage AND collection capacities are insufficient – DoD stakeholders conclude

Danielle C. Tarraf 19, William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, Ali Wyne, Daniel Elinoff, Edward Geist, Benjamin N. Harris, Eric Hui, Cedric Kenney, Sydne Newberry, Chandler Sachs, Peter Schirmer, Danielle Schlang, Victoria M. Smith, Abbie Tingstad, Padmaja Vedula, and Kristin Warren, The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations, RAND Corporation, 2019. <https://www.rand.org/pubs/research_reports/RR4229.html>, nihara

Data

The study team interviewed and collected input from many DoD stakeholders with responsibility for data and infrastructure. The team also interviewed DoD personnel who use these data and infrastructure for analytics or AI purposes. One striking aspect of our interviews was the general enthusiasm expressed for the JCF, with “wish lists” that included the development of uniform policies for sandboxing and application programming interfaces,32 the development of common algorithm libraries and repositories for open source projects, and reuse of code components and documentation of best practices (see section “Organization: At the OSD Level” in Appendix B). A notable development within DoD is the recent creation of the CDO role, with Michael Conlin in place as DoD’s first CDO as of August 2018. We anticipate that with time, the data posture of DoD will significantly evolve. Nonetheless, through our interviews, we identified several serious obstacles and impediments in regard to data at present.

Data are not collected and stored at every opportunity. DoD’s software infrastructure exists in an environment in which storage space remains a scarce resource and many opportunities to record data are missed. Even if modern storage infrastructure capacities were acquired, additional barriers might prevent the mass collection and storage of data. In particular, DoD still faces significant constraints on network bandwidth, which can hamper the ability to move data collected from sensors in the field to a location where they can be stored. Additionally, DoD’s suite of software was designed for and implemented in an era in which applications stored only data for which DoD had an immediate use, rather than speculatively storing data that could be mined for insights by professionals. This situation has resulted both in inadequate data storage and in storage of less-appropriate data; in addition, too much of the data collected have already been transformed from a raw, foundational form into an intermediate or aggregated result. These transformations, although an appropriate optimization at the time, strip away crucial context from information needed to train modern ML-based algorithms. Finally, outdated collection processes result in some data not being collected and digitized; recent RAND work on acquisition data within DoD illustrates this point.33

#### 2 – accessibility – it’s limited for existing data

Danielle C. Tarraf 19, William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, Ali Wyne, Daniel Elinoff, Edward Geist, Benjamin N. Harris, Eric Hui, Cedric Kenney, Sydne Newberry, Chandler Sachs, Peter Schirmer, Danielle Schlang, Victoria M. Smith, Abbie Tingstad, Padmaja Vedula, and Kristin Warren, The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations, RAND Corporation, 2019. <https://www.rand.org/pubs/research_reports/RR4229.html>, nihara

Access to existing data is limited. Several barriers within DoD present substantial obstacles to data-sharing today. First, personnel might view data as a means of retaining power or value in DoD or of protecting their work from extensive oversight, and therefore those personnel resist data-sharing. Additionally, many data owners resist sharing their data out of security concerns and the worry that another organization might suffer a security breach. Finally, the security clearance process and other bureaucratic procedures can introduce a significant lag before an individual will be allowed to access data. This problem presents a particular difficulty in recruiting new talent into DoD, and substantially lowers productivity, even for long-standing DoD personnel. Some of these issues, as they pertain to acquisition data, were highlighted in a recent RAND report.34 Informal networks can substantially reduce the delay in gaining access to data, but based on our interviews, these workarounds appear to be haphazard.

#### 3 – interoperability – it’s are inconsistent – establishing relationships across data collected by different systems is impossible, turns case

Danielle C. Tarraf 19, William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, Ali Wyne, Daniel Elinoff, Edward Geist, Benjamin N. Harris, Eric Hui, Cedric Kenney, Sydne Newberry, Chandler Sachs, Peter Schirmer, Danielle Schlang, Victoria M. Smith, Abbie Tingstad, Padmaja Vedula, and Kristin Warren, The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations, RAND Corporation, 2019. <https://www.rand.org/pubs/research_reports/RR4229.html>, nihara

Lack of interoperability in systems across DoD creates challenges. Interoperability of data collected by different systems, even within the same functional domain, remains a problem. Software applications within DoD have not typically been designed to work with other DoD applications—even applications in the same functional domain. Consequently, establishing relationships between data collected by one system and data collected by another can be virtually impossible. Even worse, it appears that DoD leadership is often presented with inconsistent values originating from different systems for the same data point, undermining leadership’s willingness to trust data from DoD systems or make decisions based on data at all (see section “Data” in Appendix B).

#### 4 – traceability AND comprehensibility – collection does NOT include context – makes leveraging it impossible – NO implementation of algorithms

Danielle C. Tarraf 19, William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, Ali Wyne, Daniel Elinoff, Edward Geist, Benjamin N. Harris, Eric Hui, Cedric Kenney, Sydne Newberry, Chandler Sachs, Peter Schirmer, Danielle Schlang, Victoria M. Smith, Abbie Tingstad, Padmaja Vedula, and Kristin Warren, The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations, RAND Corporation, 2019. <https://www.rand.org/pubs/research_reports/RR4229.html>, nihara

The data that exist are not always understandable or traceable. DoD systems frequently lack the documentation or metadata required to provide context as to what particular data actually mean or how they were generated. For example, an Army database might store a numeric value for the number of tanks at a particular facility, but it might not explain whether this number indicates all functional tanks, all tanks assigned to a particular unit, or all tanks of any status present at the location. Other data values with less descriptive names will frequently be even more difficult to comprehend and use. The lack of any centralized tool for data service means that it is difficult for DoD personnel, even in leadership, to discover what data might be available to inform a question. Instead, discovering new data sources and interpreting them typically requires personal networks or other informal mechanisms.

In sum, all indications are that DoD data are not currently being used to their full potential. Overall, the problems we noted here represent a formidable obstacle to implementing AI algorithms,35 even at the level of enterprise AI. Both Project Maven and the JAIC’s preventative maintenance prototype have found that issues around data quality and availability are a primary barrier to progress (see section “Data” in Appendix B). These issues, if left unresolved, will continue to hamper the development and deployment of AI throughout DoD. Additionally, we highlight the following friction point.

#### 5 – ambiguity – directly implicates any external OR private sector involvement – pilot projects that collaborate with industry fail AND are NOT operationalizable because of data ownership vendor lock

Danielle C. Tarraf 19, William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, Ali Wyne, Daniel Elinoff, Edward Geist, Benjamin N. Harris, Eric Hui, Cedric Kenney, Sydne Newberry, Chandler Sachs, Peter Schirmer, Danielle Schlang, Victoria M. Smith, Abbie Tingstad, Padmaja Vedula, and Kristin Warren, The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations, RAND Corporation, 2019. <https://www.rand.org/pubs/research_reports/RR4229.html>, nihara

There is ambiguity in data ownership where external vendors are involved. In theory, data that originate in DoD should be owned by DoD. In practice, when DoD data are analyzed or otherwise worked on by external vendors, the ownership of the data, albeit in a new modified form, becomes murky. This issue was highlighted in recent unpublished RAND work addressing weapon system intellectual property and data rights. This ambiguity of ownership leads to multiple problems beyond the specific ownership and potential loss of control of the data, including vendor lock to retain use of the data, the inability to aggregate data across multiple vendors, and the inability to use the data for additional internal purposes, among others. Although this problem is not unique to DoD, as some of our industry interviewees described (see section “Industry: Data” in Appendix C), it is one that DoD also needs to come to terms with.

#### AND, talent:

#### DoD can’t define OR track it – NOR cultivate it

Danielle C. Tarraf 19, William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, Ali Wyne, Daniel Elinoff, Edward Geist, Benjamin N. Harris, Eric Hui, Cedric Kenney, Sydne Newberry, Chandler Sachs, Peter Schirmer, Danielle Schlang, Victoria M. Smith, Abbie Tingstad, Padmaja Vedula, and Kristin Warren, The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations, RAND Corporation, 2019. <https://www.rand.org/pubs/research_reports/RR4229.html>, nihara

DoD lacks clear mechanisms for defining and tracking AI talent. This situation is because of the lack of an AI workforce classification and the lack of consensus on the definition and requisite skills of an AI worker. Currently, the technical AI talent that exists is being placed inconsistently in military and civilian occupational specialties.

For example, our interviewees across the services noted that civilian AI talent is found across occupations, including operations researchers, program analysts, scientists, software developers, and engineers. On the uniformed side, the Army and Navy are actively considering a new occupational specialty for servicemembers just for AI, but the Air Force and Marines are not. Adding to this complicated picture, some existing uniformed and civilian occupations that might have a role to play in developing AI technologies, such as software engineers, are classified as cyber talent (see section “DoD Posture for Cyber” in Appendix D). On this note, although it is not prevalent, we observed an inclination among some of our interviewees to view AI, software, cyber, and data science as somewhat interchangeable, particularly with regard to technical talent.37

DoD struggles to grow and cultivate AI talent. Our interviews suggest a mixed appreciation for what technical AI talent consists of and which AI talent is needed. Several entities we interviewed, such as the service labs, had a clear sense of AI talent needs, but the majority were still in the beginning stages of such considerations and were more likely to emphasize contracting out for technical talent. Moreover, for those that were clear on AI talent needs, it was a challenge to define the exact knowledge, skills, and abilities they perceived that were required. Ultimately, the AI talent needs of DoD (type,38 quantity, and mix) will depend on the broader strategy pursued for scaling AI, and the extent to which scaling AI will rely on the development of products in-house as opposed to through contracting and outsourcing. The skill sets needed for development of products in-house are significantly different from those needed for contracting and outsourcing, though all AI talent (technical or managerial) is difficult to access in the present market. Nonetheless, the consensus is that DoD faces stiff competition for AI skills and expertise, as evidenced by our interviews across academia, industry, and DoD.39 Many of our DoD interviewees discussed the challenges related to attracting and recruiting technical talent more generally, and expressed the belief that AI talent would be no different. In that spirit, we point to a recent RAND study on career paths for data scientists within the Defense Intelligence Agency.40 Interviews across DoD cited intense competition with the private sector, the limited ability to compete on salary, and long hiring processes. At the same time, the majority of our interviewees were optimistic that DoD could compete well on mission and the opportunity to work on important and interesting problems (see section “Talent” in Appendix B, and section “Thoughts Across Industry: On DoD Competing for AI Talent” in Appendix C).41 We note that similar themes to the ones we highlight here appear in the DIB’s SWAP study, even as we reemphasize that AI is not software.42

Overall, the services generally acknowledged the need for greater permeability of technical talent between civilians and uniformed services.43 Several interviewees expressed the belief that they need to exploit existing authorities for civilians to do a tour of duty for several years at DoD, with one noting they would be more than happy to take technical talent that was “burned out” in industry or academic jobs and wanted a change. This idea complements what we heard from industry and academia, where a variety of mechanisms are used to support external activity of employees in the interests of retaining them (see section “Academia: Talent” in Appendix C, and section “Industry: Talent” in Appendix C). Interviewees also described retention efforts for current service members with technical skills; these efforts leverage existing programs that enable some degree of permeability. This process includes formal training and rotation opportunities for officers in technical disciplines through established partnerships with industry and academia.44 A recent congressionally mandated RAND study catalogues more examples of such rotation programs.45 Regardless of the approach taken, if DoD is to be successful in scaling AI, it needs to ensure it has access to some level of AI talent, both technical (R&D) and managerial (acquisition), and that the talent that exists maintains its knowledge and skills in a fast-changing technical environment. DoD also needs to cultivate respect of and promotions for military personnel involved in AI activities and to compete in an AI talent market in which individuals expect change (in jobs and employers) every few years.

### no ai

#### Overhyped expectations causes inevitable “AI winter” – which draws funding and investments away from R&D. Independently, defense officials resist integration

Julia Ciocca et al 21, Michael C. Horowitz, and Lauren Kahn, Julia Ciocca is a Research Fellow at Perry World House at the University of Pennsylvania. Michael C. Horowitz is Richard Perry Professor and Director of Perry World House at the University of Pennsylvania. Lauren Kahn is a Research Fellow at Perry World House at the University of Pennsylvania. 4-6-2021, "The Perils of Overhyping Artificial Intelligence," Foreign Affairs, <https://www.foreignaffairs.com/articles/united-states/2021-04-06/perils-overhyping-artificial-intelligence>, nihara

In 1983, the U.S. military’s research and development arm began a ten-year, $1 billion machine intelligence program aimed at keeping the United States ahead of its technological rivals. From the start, computer scientists criticized the project as unrealistic. It promised big and ultimately failed hard in the eyes of the Pentagon, ushering in a long artificial intelligence (AI) “winter” during which potential funders, including the U.S. military, shied away from big investments in the field and abandoned promising areas of research.

Today, AI is once again the darling of the national security services. And once again, it risks sliding backward as a result of a destructive “hype cycle” in which overpromising conspires with inevitable setbacks to undermine the long-term success of a transformative new technology. Military powers around the world are investing heavily in AI, seeking battlefield and other security applications that might provide an advantage over potential adversaries. In the United States, there is a growing sense of urgency around AI, and rightly so. As former Secretary of Defense Mark Esper put it, “Those who are first to harness once-in-a-generation technologies often have a decisive advantage on the battlefield for years to come.” However, there is a very real risk that expectations are being set too high and that an unwillingness to tolerate failures will mean the United States squanders AI’s potential and falls behind its rivals.

ACCIDENTS HAPPEN

The path to the effective uses of military AI will inevitably be rocky, with accidents and missteps amplified by overhyping of the sort that has seen, for example, outsize excitement over futuristic, fully autonomous cars give way to the mundane reality of vehicles that can just about parallel park. A mismatch between expectations and reality can spell the end for new technologies and is especially likely to do so when governments prioritize quick wins over long-term potential. Successful AI adoption will require patience and careful communication so that opportunistic naysayers cannot hold up accidents as proof that failure is inevitable.

AI might be especially vulnerable to this type of hype-induced backsliding. It has suffered two previous winters in its relatively short history, during which AI’s failure to live up to expectations drove declines in funding and interest. AI is also tricky to understand and to define, and the algorithms on which it is based are prone to failure when used outside the context of their initial development.

Incorporating AI into the U.S. military, moreover, will require disruptive changes to everything from force structure and promotion patterns to doctrine and responsibility. This will inevitably trigger resistance. And because U.S. defense officials generally lack the expertise to assess AI advances currently being driven by the private sector, opponents of the new technology will find it easier to capitalize on inevitable setbacks, arguing that a potentially effective application of AI is not just too early but will never materialize.

Yet the naysayers cannot be allowed to triumph. Over and over throughout history, resistance to technological change has come back to haunt militaries. In the late nineteenth century, for instance, France’s navy sought to counter British naval supremacy by investing heavily in submarines and torpedo boats. The technology of the time was not up to the task, however, and France reverted to building battleships, a move that left the United Kingdom to rule the waves until the outbreak of World War II.

About 25 years later, Russia abandoned early design armored vehicles because they got stuck in the mud. Better tread and more power were the simple fixes. But instead, Russia put off procurement of the vehicles and fell behind as others moved forward. In short order, the armored vehicle evolved into the tank, a critical innovation in ground warfare. The Russians, like the French, ought to have shown more patience and persistence.

#### No adoption – commercial development gaps, inefficient testing, AND resistance to deployment

Julia Ciocca et al 21, Michael C. Horowitz, and Lauren Kahn, Julia Ciocca is a Research Fellow at Perry World House at the University of Pennsylvania. Michael C. Horowitz is Richard Perry Professor and Director of Perry World House at the University of Pennsylvania. Lauren Kahn is a Research Fellow at Perry World House at the University of Pennsylvania. 4-6-2021, "The Perils of Overhyping Artificial Intelligence," Foreign Affairs, <https://www.foreignaffairs.com/articles/united-states/2021-04-06/perils-overhyping-artificial-intelligence>, nihara

STUMBLING BLOCKS

There are three main chokepoints at which new technologies such as AI often fall short of inflated expectations and therefore backslide into the abyss of premature abandonment. The first is the “valley of death,” the appropriately named gap between a technology’s development in the private sector and its acquisition by governments or militaries, which often require more certainty than developers can offer. It is the burial ground for many great ideas.

If the valley of death is safely navigated, a cumbersome and timid testing and evaluation process can be the next trap. The U.S. Department of Defense in particular needs to invest in making testing, evaluation, verification, and validation of new AI applications more efficient. Existing processes are not designed to handle ever-evolving machine learning systems and AI algorithms, which may enable the deployment of unreliable systems. These, in turn, are more likely to fail, generating mistrust and resistance to further AI adoption.

The final hurdle is real-world deployment. Fear of the many unknowns—such as the perceived impact on soldiers—could strengthen resistance to the broad integration of AI over time, as could the perception that AI will reduce the human role in warfare. These are fertile grounds for those looking to seize upon AI errors in order to halt the technology’s use.

.

### No escalation

#### Russia already attacking NATO countries---Proves Article 5 won’t get triggered

Matthew Holroyd 22, Correspondent for Euronews. “Ukraine war: False claims spread about military movements in Poland and Finland” June 05. <https://www.euronews.com/my-europe/2022/05/06/ukraine-war-false-claims-spread-about-military-movements-in-poland-and-finland> //barn

Online misinformation about the armies of Poland and Finland has circulated online amid Russia's invasion of Ukraine.

Social media users have falsely suggested that both European Union member states are preparing to enter the war or engage in military conflict.

Investigations by Euronews and other independent fact-checkers have revealed that the claims are false and alleged video evidence has been taken out of context.

In times of conflict and crisis, when people are hungry for details about the war, misinformation can be equally as viral as verified facts.

Both Moscow and Kyiv have used social media to spread their propaganda, while pro-Kremlin users have also spread false claims.

Poland is NOT preparing to invade Ukrainian territory

A recent viral video has falsely claimed that Poland is preparing to send troops into Western Ukraine to confront Russia.

The footage -- which includes the logo and branding of BBC News -- alleges that Poland's military general Yaroslav Mika had signed an order to put army sections on “full alert”.

The video was shared online by users in a number of languages, including Czech, French, Italian, Polish, Russian, and Turkish.

But online searches show no record of the BBC ever producing a report on the story, and senior disinformation journalists at the company state that the video is "fake".

The branding of the BBC was also previously used to spread false claims about military strikes on a Kramamtorsk railway station that killed dozens of people.

Poland has led calls for the EU to toughen sanctions on Russia and for the NATO alliance to arm Ukraine during the war.

While Poland has provided its neighbour with military aid, it has not expressed any such plans to send troops into Ukrainian territory.

The General Command of the Polish Armed Forces dismissed the allegations and stated that any alleged order to move troops was "counterfeit".

"This is a false order of the Polish General Staff, the whole document is fake," its official Twitter account said.

Kremlin spokesperson Dmitry Peskov said on Friday that hostile rhetoric was coming out of Poland and suggested that Warsaw could be "a source of threat".

Polish government officials say Moscow and pro-Kremlin social media users are now launching information attacks against the country.

"The fake order of the Polish general, created for propaganda purposes, was used for disinformation activities against Poland," said Stanisław Żaryn, a spokesman for Poland's Special Services Ministry.

"The order was used to legitimise insinuations about Poland's plans to attack western Ukraine," he said on Twitter.

"[These] are all elements indicating that Russia is conducting a coordinated information operation against Poland."

Warsaw says it has recently stepped up efforts to combat the spread of "disinformation" being spread by Russia.

### FDPR card for ADV CP

* The USFG should impose FDPR export controls on Russia [needs to be edited obv]

#### FDPR controls incapacitate Russian AI

Allen Maggard and Edrin Spahiu 22, s currently a graduate student at American University’s School of International Service. Previously, he worked for the US Department of Justice’s Foreign Corrupt Practices Act unit, TD International (a due diligence and political risk advisory firm), and the Center for Strategic and International Studies. “CAN TECH SANCTIONS DETER RUSSIA FROM WAR WITH UKRAINE?” February 22. <https://inkstickmedia.com/can-tech-sanctions-deter-russia-from-war-with-ukraine/> //barn

WHAT FDPR EXPORT CONTROLS CAN DO

Any deployment of FDPR export controls would significantly reduce the Kremlin’s ability to keep pace with the global race to capitalize on AI technologies by throttling Russia’s access to the underlying hardware that make those AI technologies possible. Insofar as AI technologies require prodigious amounts of data to function properly, they are fundamentally reliant on computer microprocessors able to manipulate massive volumes of digital information swiftly and at scale.

The Russian computer chip industry is dominated by two companies, Baikal Electronics and the Moscow Center of SPARC Technologies (MCST), both of which rely on the Taiwan Semiconductor Manufacturing Corporation (TSMC) to fabricate their chip designs. Despite its complicated role in the Biden administration’s plans to secure global semiconductor supply lines, TSMC is an important geopolitical actor in its own right by virtue of its position as the leading manufacturer of the semiconductors used by computer chip companies worldwide. Nonetheless, the FDPR’s statutory basis will likely compel TSMC and most other key points in the global semiconductor supply chain to shutter their dealings with MCST and Baikal Electronics.

In keeping with the logic of import substitution policies (importozameshchenie) adopted in response to the imposition of western sanctions following Russia’s invasion of Ukraine in 2014, the Kremlin seeks to stimulate semiconductor production capabilities to compensate for losing access to TSMC and other overseas chip manufacturers. Russian Prime Minister Mikhail Mishustin’s ambitious roadmap for this effort, first presented in January 2020, aims to curtail Russia’s reliance on international semiconductor supply chains through import substitution, competition for global chip markets, and, ideally, eventual market dominance. Putin’s October 2019 AI strategy also prescribes the rollout of domestically-manufactured microprocessors “not inferior to their global equivalents as far as speed and energy efficiency.”

RUSSIA’S AI INVESTMENTS

A handful of semiconductor fabrication facilities (fabs) already exist inside Russia. For example, in November 2021, fabs operated by Mikron — a subsidiary of Rostec, a state-owned technology company subject to US sanctions since 2014 — reportedly completed an experimental batch of the MK32 Amur, the first ever microcontroller chip entirely designed and produced inside Russia. Although fabs like those operated by Mikron require substantial capital investments over time lest they become obsolete, Russia’s international reserves currently total more than $600 billion — a sum that should enable the Kremlin to subsidize fab development and maintenance for some time. In fact, Russia plans to invest RUB 768.5 million (approximately $9.6 million in US dollars) in information technology infrastructure by 2024. These plans appear to include recruiting foreign talent. For example, in September 2021, Russian media reported that the Ministry for Manufacturing and Trade had partnered with VEB.RF (formerly Vneshekonombank) to recruit several specialists from Taiwanese semiconductor manufacturer United Microelectronics Corporation as part of an effort to relaunch a bankrupt chip plant outside Moscow.

Whether these investments will immediately translate into chipsets capable of providing the computing power AI technologies require remains an open question. A chip’s computing power is generally measured in terms of the length of its transistor gates, which govern the flow of electricity and thereby control the flow of information through a computer system. The smaller the transistor gate, the more transistors that can fit onto a single chip, thus enabling greater computing power and energy efficiency per individual chip. At the time of this writing, the most advanced mass market chips used for AI applications, such as AMD’s Radeon Instinct family of graphics processing units (GPU) and Huawei’s Ascend 910 processors, feature transistor components measuring approximately 7 nanometers (nm). By contrast, Russian media reports indicate that the components composing Mikron’s MK32 Amur microcontroller measure approximately 90 nm. For context, 90 nm chipsets provided the computing power behind the Sony PlayStation 3 upon that console’s release in November 2006. In this sense, the MK32 Amur, though ostensibly a success in terms of Russian import substitution strategies, has specifications that fall well short of US and Chinese-manufactured AI chips, which suggests that existing Russian fabs are several generations old.

Even if the Kremlin manages to parlay its international reserves into developing more advanced fabs, there is no guarantee that Russian chip companies can produce reliable designs. Russian business daily Kommersant has reported that the Ministry of Internal Affairs, among other key government organs and state-owned enterprises have encountered extensive problems with the latest generation of MCST’s flagship Elbrus family of microprocessors. According to anonymous sources familiar with the situation, the issues with MCST’s chips are so grave as to have convinced major economic actors like Rostec and Sber (formerly Sberbank) to refrain from fully embracing domestically produced microprocessors until the latter’s computing capacities become more reliable without them becoming more expensive than foreign analogues.

Minpromtorg has even gone so far as to file a civil lawsuit demanding that the Isaac S. Bruk Institute of Electronic Control Machines (IECM), MCST’s parent institution, pay back RUB 325.5 million, which is approximately $4.1 million in US dollars as of Feb. 21 2022 in subsidies along with RUB 92.3 million (approximately $1.2 million US dollars) in additional fines. Although limited information is available regarding the legal action under concern, CNews.ru reports that Minpromtorg — which has also filed similar lawsuits against Baikal Electronics and Russian supercomputer firm T-Platforms — originally extended the subsidies as part of a program to develop a massively scalable server system employing MCST’s Elbrus 8S microprocessor chip for use in the kind of data center and supercomputer equipment utilized in AI applications.

Equally debatable is the argument that sanctions will catalyze import substitution policies mitigating Russia’s reliance on imports of chips. The available evidence suggests that this is not the case: Data collected by the International Trade Center, an international development agency run jointly by the World Trade Organization and the UNs, shows that Russian import of semiconductor devices and electronic integrated circuits actually grew by 47 % and 50 % respectively, between 2014 and 2019. Russian security services observer Andrei Soldatov maintains that the Kremlin has actually made considerable progress in hi-tech import substitution since 2019; however, most of the progress that Soldatov references concerns the development of alternatives to western online platforms and other consumer-oriented applications, rather than the sort of high-caliber semiconductors required to support advanced AI functionalities.

The Kremlin could turn to Chinese semiconductor manufacturers for AI-capable chipsets, though it is by no means certain that Beijing would allow domestic chip fabricators to supply Russia — especially if it meant running afoul of FDPR controls and depriving Chinese companies of access to US technology, financing, and markets. Moreover, the notion that using Chinese technology serves the interests of the Kremlin’s AI development strategy, and its much-touted “digital sovereignty” policy more broadly, better than using US-derived analogues may be a hard sell for elements within the Russian security elite, not least given that both of the above scenarios essentially entail reliance on a foreign power for sensitive hardware.

# Aff

## Advantage Updates

### industry signaling scenario

#### Europe has unique AI talent, but needs funding to utilize it

Daniel Castro et al 19, Castro is the director of the Center for Data Innovation and vice president of the Information Technology and Innovation Foundation. Michael McLaughlin is a research analyst at the Center for Data Innovation. Eline Chivot is a former senior policy analyst at the Center for Data Innovation. “Who Is Winning the AI Race: China, the EU or the United States?” August 19. <https://datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/> //barn

The United States leads for several reasons. First, it has the most AI start-ups, with its AI start-up ecosystem having received the most private equity and venture capital funding.[3] Second, it leads in the development of both traditional semiconductors and the computer chips that power AI systems.[4] Third, while it produces fewer AI scholarly papers than the EU or China, it produces the highest-quality papers on average.[5] Finally, while the United States has less overall AI talent than the European Union, its talent is more elite.[6]

China is ahead of the European Union in AI and appears to be quickly reducing the gap between itself and the United States. It has more access to data than the European Union and the United States, which is important because many of today’s AI systems use large datasets to train their models accurately. In venture capital and private equity funding, Chinese AI start-ups received more funding than U.S. start-ups in 2017, but not in 2016 or 2018.[7] China, however, is clearly behind both the United States and the European Union in high-quality AI talent. Several European Union member states, including Italy, had more AI researchers ranked in the top 10 percent internationally than China as of 2017.[8] Nonetheless, China has made clear progress relative to the United States in most metrics, and significantly outpaces the European Union in funding and AI adoption.

The European Union has the talent to compete with the United States and China. Indeed, it has more AI researchers than its peers, and typically produces the most research as well.[9] However, there is a disconnect between the amount of AI talent in the EU and its commercial AI adoption and funding. For example, AI start-ups in the United States and China both received more venture capital and private equity funding in 2017 alone than EU AI start-ups received in the three years covering 2016 through 2018.[10] The European Union’s laggard position reduces its ability to not only enjoy the economic and social benefits of AI, but also influence global AI governance, which is a goal of the European Commission.[11]

#### Transatlantic cooperation signals a shift and solves for Chinese authoritarian internet---Current European proposals are creating an environment of uncertainty within stakeholder circles

Meredith Broadbent 21, Meredith serves as a senior adviser with the Scholl Chair in International Business at the Center for Strategic and International Studies and is a former chair of the U.S. International Trade Commission. “What’s Ahead for a Cooperative Regulatory Agenda on Artificial Intelligence?” March 17. <https://www.csis.org/analysis/whats-ahead-cooperative-regulatory-agenda-artificial-intelligence> //barn

In light of the AI white paper, it appears that the Commission is moving forward with broad, horizontal, and relatively intrusive regulation of AI applications. Ex-ante conformity assessments to control access to the EU market for AI applications originating outside of the EU are proposed. The Commission is also considering data quality and traceability requirements that would require non-EU firms to train AI applications on GDPR compliant data as a condition of market access in the European Union. Sectors that will likely be impacted by EU regulation of AI are healthcare, transportation/autos and parts producers, energy, servic­­­es that rely on consumer data, the public sector, and more.

To complement the AI white paper, the European Commission released a set of documents on the regulation of AI, including:

Communication on a European Strategy for Data, in which the Commission outlined the importance of data for economic development and the decision to invest in High Impact Projects to fund “AI ecosystems” related to the development of data spaces and cloud services;

Shaping Europe’s Digital Future, in which the Commission itemized all key actions to be undertaken by the European Union in order to ease data flow across the Union while enacting proper regulation to maintain the strength of democratic institutions and free-market competition, especially in developing sectors such as AI and cryptocurrency; and

Report on the Safety and Liability Implications of AI, the Internet of Things and Robotics, in which the Commission reviews gaps in product safety legislation that do not adequately address risks such as cyberattacks due to connectivity, autonomous behaviors of products, faulty data, opacity of algorithmic systems, software updates, and complex safety management and value chains.

Of the four major documents, the AI white paper has attracted the most interest from stakeholders. Many are concerned that the Commission’s regulatory vision will be burdensome, unworkable, and have the result of suppressing the success of European digital start-ups and the innovation ecosystem in Europe. Digital rights groups, for their part, have raised alarm over the Commission’s decision to not include a proposal for a three to five-year moratorium on facial recognition technology in the white paper.

The United States and Europe, which both face the same threat of growing authoritarian dominance of the internet by China, could build a valuable strategic partnership that would support the scaling of AI capabilities of Western economies.

#### Testing and Interoperability are key concerns for stakeholders

Meredith Broadbent 21, Meredith serves as a senior adviser with the Scholl Chair in International Business at the Center for Strategic and International Studies and is a former chair of the U.S. International Trade Commission. “What’s Ahead for a Cooperative Regulatory Agenda on Artificial Intelligence?” March 17. <https://www.csis.org/analysis/whats-ahead-cooperative-regulatory-agenda-artificial-intelligence> //barn

Responding to Commission plans to enact stricter rules for high-risk AI technologies, such as compliance tests and controls, 14 EU member states published a paper outlining their position urging the Commission to adopt a “soft law approach” consisting of “self-regulation, voluntary labeling and other voluntary practices, as well as a robust standardization process as a supplement to existing legislation that ensures that essential safety and security standards are met.”1 The countries recommend a European approach to AI regulation in which innovation and trustworthiness work together in a “coherent and borderless single AI market.”

For several reasons, AI giants such as Google and Facebook, as well as startups, tech companies, and associations, have raised concerns that meeting regulatory requirements considered in the AI white paper will stifle innovation and may require actions that breach EU data privacy rules.

First, technology corporations are waiting anxiously to see how the Commission will define “high-risk” AI, as that will have a foundational impact on how AI regulation is implemented. A chief concern is that the Commission’s definition of “high-risk” AI and its approach to the concept is too broad and would result in one-size-fits-all regulation for all AI applications in “high-risk” sectors, regardless of differences between the sectors and the type of AI application. Instead, Google, Facebook, and Digital Future for Europe, which represents associations, tech companies, and startups from the Digital Nine,2 propose a sector, technology, or application-specific regulatory approach that takes into account unique risks posed by individual sectors as well as the application itself. For example, risks posed by AI applications in the healthcare sector are much different than those in the transportation sector. One-size-fits-all regulation for AI applications within sectors would also be suboptimal. An AI chatbot developed for a healthcare company to better understand patient needs presents a different level and type of risk than an AI application involved in medical decision-making.

Although expressing agreement with several aspects of the white paper, IBM, one of the largest technology employers in the European Union, argues that existing sector-specific governance structures would be better suited to implement regulation to avoid unnecessarily impeding AI development. For example, the Commission’s propositions on human oversight requirements may be inappropriately restrictive in the context of automated driving, since “it is impossible to oversee every single decision taken by an automated car, due to most decisions being taken in real time.”

Stakeholders have also raised concerns over vague exceptions included in the white paper that could make it difficult to determine whether an AI application is subject to “high-risk” rules. The inclusion of AI applications that could cause “immaterial damage” as a factor in determining risk was characterized as nebulous by many stakeholders. The white paper also suggests that there may be “exceptional circumstances” where an AI application could be considered “high-risk” regardless of its sector. Booking.com, an online travel agency headquartered in the Netherlands, has questioned the white paper’s unspecific notion that “applications affecting consumer rights” could also be required to apply “high-risk” rules. These exceptions and ambiguities inject an uncertainty into which AI applications will be considered “high-risk” and increases expectations that the Commission will adopt an overly broad view of “high-risk” AI applications, subjecting applications to onerous regulations that are not justified. In comments to the white paper, the European Digital SME Alliance, a network of associations representing more than 20,000 European small and medium ICT enterprises, added, “[s]mall companies are the first to suffer from rules that are up to interpretation.”

Digital Future for Europe maintains that the “risk assessment process would stifle many AI innovations before they have developed,” and through ex-ante regulation “the EU threatens to skew the whole development of European AI.” Additionally, IBM has cast doubt upon the white paper’s proposal of an explicit and exhaustive list of sectors in which “high-risk” applications could emerge, due to the rapid evolution of AI technology and its diverse applications.

Second, companies have raised concerns regarding the requirement that AI developers would need to retrain AI systems in the European Union to meet data set requirements. Facebook and Google note that restricting data available to train AI to just EU data is likely to reduce the quality of the AI product and contribute to biases in the systems. Digital Future for Europe suggests the Commission focus on increasing the pool of data acceptable to regulators and available to AI developers in order to improve AI applications and encourage innovation. IBM opposes input-specific requirements, arguing instead that “high-risk” applications should be required to ensure a specific outcome, such as the absence of discrimination. The Commission’s approach to training data either wrongly assumes AI applications employ a static data set or raises the prospect that AI systems would need to be re-audited on a regular basis. That would drastically slow the ability to update and improve AI tools. This is particularly concerning if an AI application is producing undesirable or suboptimal outcomes based on a previously audited data set. Facebook has pointed out that it is unclear what data needs to be “EU data” and how the service being provided by an AI application changes that consideration. Google, as well as the European Association of Automotive Suppliers (CLEPA), worry that it is difficult to separate out the provenance of some parts of training datasets in certain fields, which often rely on third-party and open-source data. Leaving out these data sets in training could seriously hurt the quality of AI systems subsequently released in the European Union.

Third, Google and Facebook have raised concerns that compliance with rules for “high-risk” could run counter to EU privacy rules, including GDPR. Facebook worries that the proposed requirement to store training data sets could “create a direct tension” with policies to protect users’ data, such as those related to data minimization and data retention. The social media platform also worries that the proposed requirement could prohibit federated learning and other AI approaches intended to protect privacy.3 In Facebook’s view, this requirement could undermine the potential effectiveness of federated learning in protecting users’ privacy.

Requirements around algorithmic fairness and the need to share source code also appear to be in tension with EU privacy rules. Google believes that the requirement to ensure that data sets are “sufficiently representative” contrasts with GDPR obligations: “developers should not be able to access attributes such as ethnicity and therefore could not test for ethic [sic] representation in a dataset.” Google stresses that “sufficiently representative” should be more clearly defined.

As an alternative to ex-ante conformity assessments that can be burdensome, unpredictable, and could expose companies to breaches in privacy rules, Facebook and Google propose benchmark tests tailored to specific high-risk applications to determine whether or not AI will behave in a way that is expected. This approach would hold industry players accountable for mitigating bias in AI, allow internal testing of AI systems, and support a self-certification process. Digital Future for Europe suggests an overall regulatory approach that encourages responsible adoption of AI before introducing onerous regulation. To do so, European governments should open public data sets, provide for data interoperability between government data sets, refit existing European legislation to account for AI, and make sure that any new AI rules are agile and flexible. Google proposes a “large central dataset” that developers could access to protect against developers attempting to overfit models to accord with EU rules

#### Transatlantic cooperation solves innovation and adoption within Europe---Collaboration promotes more skills, education, and ease of access for companies and governments

Meredith Broadbent 21, Meredith serves as a senior adviser with the Scholl Chair in International Business at the Center for Strategic and International Studies and is a former chair of the U.S. International Trade Commission. “What’s Ahead for a Cooperative Regulatory Agenda on Artificial Intelligence?” March 17. <https://www.csis.org/analysis/whats-ahead-cooperative-regulatory-agenda-artificial-intelligence> //barn

Emerging AI Cooperation Efforts

BENEFITS OF TRANSATLANTIC COOPERATION

It will be important for the Commission to recognize that transatlantic cooperation can provide Europe with the means necessary to achieve its AI innovation and adoption goals in several key areas. First, considering the United States and the European Union together make up roughly 50 percent of global GDP and around 770 million people, establishing agreed-upon standards for making public data sets available can significantly increase European businesses’ and researchers’ access to more data. It is important that this cooperation includes clarifying where GDPR allows data sets to be shared, an area of uncertainty that carries many risks for U.S. companies. Second, reviewing laws that govern copying data sets would increase clarity about when a company is permitted to retrain and share data.

Third, collaboration will promote the scaling up of skills and education, as both the United States and the European Union can tap into a larger pool of talent, resources, academia, and institutions. While some U.S.-EU AI-related research currently exists, the projects are relatively “ad hoc and materialize within existing scientific and technological research agreements and roadmaps.” For example, the United States remained the leading non-EU participant in Horizon 2020, the European Union’s six-year research framework to implement and fund high-level EU policy initiatives, but there is significant room for increased collaboration. Right now, U.S. collaborative links with Horizon 2020 projects are only found in 2 percent of AI-related projects, 4 percent of machine learning-related projects, and 12 percent of deep learning projects.

AI features “winner-takes-most” dynamics in many industries, with companies that adopt widespread AI technology are often the quickest to reap the biggest benefits. The 10 percent of European companies that are the most extensive users of AI to date are likely to grow three times faster than the average firm over the next 15 years. MGI observes that this “winner-takes-most” dynamic applies across many countries.

It will be important for the Commission to recognize that transatlantic cooperation can provide Europe with the means necessary to achieve its AI innovation and adoption goals in several key areas.

#### Innovation and collaboration are key to stop Chinese challenging of global democracy---otherwise they take the lead and steal our innovation

Joshua Meltzer and Cameron Kerry 21, Joshua’s a Senior Fellow in Global Economy and Development for Brookings. “Strengthening international cooperation on artificial intelligence” February 17. <https://www.brookings.edu/research/strengthening-international-cooperation-on-artificial-intelligence/> //barn

The U.S. is the world leader in AI. Its strength in AI has been built on a global, open, and distributed system of innovation. However, this leadership is being challenged on two main fronts. The first is from China, which has targeted development of strong AI capacity as a strategic and economic priority and source of global power. China has benefited from global cooperation on AI research and has expanded domestic innovation capacity. At the same time, China combines a restricted domestic market with an international approach to AI that includes aggressive acquisition of intellectual property (IP) and innovation from rivals, government subsidies that tilt the playing field towards Chinese companies, and strategic engagement in international forums for standards and norms that support China’s applications of AI. These tactics are often at odds with the interests of the U.S. and other leading economies, and the use of AI in applications like repressive surveillance is at odds with American values and those of other democracies.

The second challenge comes from other governments whose AI policies could lead to prescriptive regulation that may stifle AI innovation and discriminate against U.S. technology firms. Such policies also disregard the global nature of AI development. Without international coordination and integration, AI policies are unlikely to realize their potential and instead create barriers to AI diffusion globally.

#### AI cooperation and investment solidify a democratic digital society and counter Chinese rise---Tech leadership IS normative leadership

Eileen Donahoe 21. Eileen is the Executive Director at Stanford Global Digital Policy Incubator. Eileen previously served as the first US Ambassador to the United Nations Human Rights Council in Geneva. “System Rivalry: How Democracies Must Compete with Digital Authoritarians” September 27. <https://www.justsecurity.org/78381/system-rivalry-how-democracies-must-compete-with-digital-authoritarians/> //barn

An essential point here: We do not need new principles. Rather, we need to reinforce confidence in the continued relevance and applicability of existing international human rights law framework — which is globally recognized and has the status of international law. That said, we do need to undertake the hard work of articulating how to adhere to our existing international human rights framework in practice, in a radically changed digital context. A global multistakeholder process must be initiated to resolve disagreements among democratic actors about the legitimacy of different data practices, platform regulations, and applications of AI-enabled tools. Rebuilding the democratic alliance around a shared understanding of how to adhere to international human rights law in digital society should be treated as a strategic priority, on par with cybersecurity and more traditional dimensions of national security.

Last, but not least, democracies need to recognize that normative leadership and technological leadership go together. If our goal is to spread democratic values rather than authoritarian norms, we must lead in technological innovation, particularly in AI and quantum computing. Dominance in those realms will translate into leverage and influence in normative realms and tech standard setting bodies. In addition, we need to become far more proactive in exporting democratic digital infrastructure as part of our trade and economic development aid programs, rather than ceding the opportunity to China to embed values into digital infrastructure in the developing world.

\* \* \*

In sum, domestic practices, international norms, and technology innovation and standards are intertwined with digital governance systems. The strength of the digital authoritarian model stems from the fact that these elements are working in tandem. Democracies must recognize these interdependencies and demonstrate leadership in all three realms, simultaneously and in a coordinated fashion.

The tech practices we showcase in our domestic context, the norms for which we advocate in international tech fora, and the investments we make in emerging technologies and democratic information infrastructure will be mutually reinforcing. If this complex set of tasks is embraced and tackled with the sense of urgency and purpose it deserves, a prosperous, secure democratic future can be solidified. These are the essential elements from which we can build a democratic digital society.

### ukraine scenario

#### NATO Interoperability thwarts Russian attacks in Ukraine---AI data collection and logistics are vital to training and battlefield tactics as well as countering cyber-attacks before they escalate

Dr. Sanur Sharma 22, Researcher working as Associate Fellow at MP-IDSA. Dr. Sharma’s research area includes Artificial Intelligence, Social Media Analytics, Machine Learning and Information Security. "NATO’s AI Push And Military Implications – Analysis" May 30. <https://www.eurasiareview.com/30052022-natos-ai-push-and-military-implications-analysis/> //barn

NATO’s AI Influence in Russia–Ukraine Confrontations

AI has been a contributing agent in weaponising cyberspace and augmenting cyberwarfare to the next level in modern battlefield scenarios. While some of its uses such as in scaling of data analytics, data fusion, deep fakes, cyber defence have matured, its use in autonomous weapon systems and other complex operational applications are at a nascent stage.

AI has been aggressively used to spread disinformation in the Russia–Ukraine War. Machine learning algorithms have been used to amplify misleading and fake content on social media platforms, like doctored videos of invading forces and fake live streams. On the other hand, it has also been used for anomaly detection, identification of disinformation and for cybersecurity. AI uses natural language processing algorithms, machine learning and deep learning to identify anomalies in the text data, images and videos.

Russia is said to have used AI-enabled systems not only on the battlefield but also in cyberspace, targeting the critical infrastructures of Ukraine.11 Russian troll farms have been alleged to have used AI-enabled systems to generate human faces for fake propagandist personas on social media platforms like Twitter, Instagram and Facebook.12 NATO countries have also used AI to help Ukraine counter such AI-based attacks. Private companies are also playing a role in the unfolding AI battlespace. US-based companies like Snorkel AI, a data science platform, has made its services accessible to federal authorities for the detection of anomalous signals and adversary communications in order to access high-value information for better decision-making.13

Similarly, Ukraine has been given free access to Clearview AI facial recognition software, which has a database of 2 billion photos crawled from Russian social media platforms. This software is being used for the detection of Russian forces and to identify the dead and gauge the spread of disinformation in cyberspace.14 AI’s analytical potential has been tapped by companies even before the Russia–Ukraine war started. In December 2021, a geospatial data firm, SpaceKnow, claimed to have detected a military presence in Yelna, a Russian town.

The Russia–Ukraine conflict has become a test case for AI adoption in modern warfare. The US is using the conflict as a test-bed for many of its AI projects with the Pentagon’s ‘Maven’ project having contributed to the detection and classification of objects of interest from various drone footage through AI and Machine Learning (ML) algorithms. It has been reported that the Pentagon has been using AI and ML tools to collect a vast amount of data on the Russia–Ukraine war and analyse it to learn and generate battlefield intelligence about the Russian command and control strategies.15

The advanced AI-enabled systems with the US Department of Defense (DoD) are said to have been used for overseeing the battlefield and collecting and archiving signals intelligence. It was stated at the Defense One’s Genius AI Summit in April 2022 that all this information will be fed into systems for training of machine learning algorithms to support future decision-making processes.16 It is believed that the US and NATO allies have already built such AI-enabled cyber weapons and defences, information about which is said to be highly classified.17

The US DoD and its allies have taken advantage of these advanced tools to gather critical information from the publically available image data to thwart Russian attacks in Ukraine. This war data will also help NATO allies anticipate adversary attacks, their behaviour, and the use of advanced technologies in the real world by countries like China and Russia. This intelligence will also augment multifactor analysis and modelling changes dynamically by integrating different technological platforms.

Due to the sanctions imposed on Russia as a result of the Russia–Ukraine war, its AI development is expected to slow down. The ongoing conflict highlights the constraints around the use of AI. Despite AI-enabled cyber-attacks and misinformation campaign by Russia, Ukraine has mounted effective counter-cyber operations.18 Russia’s limited use of AI in the conflict can be explained through the existing vulnerabilities in the AI systems that can be exploited in many ways. One hypothesis for Russia’s limited use of AI could be the trust in such systems where it is a matter of lives and military objectives at stake.19

The vulnerabilities in the AI systems can include data poisoning and input attacks, attacking the supply pipelines by simply crafting data and feeding it to public resources, white-box and black-box attacks.20 There is always a chance of orchestrated and conflicting data in the face of AI models to derail them and to exploit the vulnerabilities in the algorithms, and active manipulation by the adversaries can be induced.

Defense Advanced Research Projects Agency (DARPA) has launched a Guaranteeing AI Robustness against Deception (GARD) programme. Under this programme, development efforts are being made to establish a theoretical foundation for defensible ML and the creation and testing of such systems.21 The Army Research Laboratory (ARL) is working with the Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA) to explore the use of ML and intelligent technology on the battlefield and strengthen the collaboration between autonomous actors and human soldiers in combat. They are also working on methods to understand the challenges of AI-enabled systems employed on the battlefield and to make them less susceptible to attacks.22

AI technology in modern warfare will be an intractable weapon in future conflicts beyond Ukraine. Countries trying to achieve a technological edge over others have started considerable investments in AI technology to strengthen their militaries. NATO has invested US$ 1 billion to develop new AI defence technologies. The US DoD has also planned to invest US$ 874 million in AI-related technologies as a part of their army research and development budget (federal fiscal year 2022 DoD budget).23 The UK DoD is funding suppliers to work with Defence Science & Technology Lab (Dstl) on AI projects which were £7million for the year 2021/22 and is supposed to increase to £29 million in the next year.[24](https://www.idsa.in/issuebrief/natos-ai-push-and-military-implications-ssharma-240522#footnote24_sxbrlaa)

NATO’s AI Adoption: Challenges and Limitations

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.

#### Ukraine is a unique opportunity for NATO to ensure interoperability in Artificial Intelligence to stop escalation due to bad crisis decision-making

Benjamin Jensen 22, Senior Fellow, Future War, Gaming, and Strategy, and International Security Program. “The Coming Storm: Insights from Ukraine about Escalation in Modern War” May 26. <https://www.csis.org/analysis/coming-storm-insights-ukraine-about-escalation-modern-war> //barn

Crises such as Ukraine will become more acute and risk prone over time without investing time and resources into understanding competition and escalation for the twenty-first century. Strategy must start with problem framing and creating a clear description of the ends, ways, and means within the context of a crisis in a manner that allows for clear-eyed assessments of how to achieve a competitive advantage. This process starts with reimagining competition, crises, and escalation in the twenty-first century.

First, the larger national security community needs new models and ways of thinking about deterrence, competition, and risk. Current defense planning and academic analytical frameworks are the legacy of Cold War dynamics that may not match a new era of competition. Unlike the Cold War, nuclear-armed states in a multipolar world will likely use nonnuclear weapons (e.g., cruise missiles, space capabilities, and cyber operations) to produce strategic effects.20 Beyond capabilities, these studies should bring the individual back in and assess risk attitudes.

Alongside efforts to think about coercion and cross-domain aspects of deterrence, the national security community needs more policy-relevant research that brings individual decisionmaking and attitudes toward risk back into how it thinks about great power competition.21 In particular, strategic analysis needs more crisis simulations and wargames designed as survey experiments to capture how both individuals and groups respond in different scenarios prone to competitive pressure, fog, and friction.22 These survey experiments enable researchers to bridge the insights of Carl Von Clausewitz’s on war, Thomas Schelling on deterrence, and Daniel Kahnmann on decisionmaking. These studies should put competition front and center and integrate new data and analytic techniques to understand competitive dynamics in a connected world.

For integrated deterrence to be more than a bumper sticker, the Department of Defense will need to initiate a new wave of research that evaluates if and how alternating capabilities—to include the emergence of Joint All-Domain Command and Control (JADC2)—and partner networks affect crisis decisionmaking. These studies will need to create alternative scenarios that reflect whether promised technological capabilities and advances in artificial intelligence and machine learning materialize, as well as the degree of partner political interests and interoperability. In other words, the national security community needs to revitalize strategic studies for the twenty-first century and integrate best practices from social science, as opposed to relying on thin case studies and broader—and often untestable—generalizations about war.

#### Ukraine reinforces uniqueness for collaboration and norms

Margarita Konaev and Tate Nurkin 22, Research Fellow & Research Analyst, Center for Security and Emerging Technology, Georgetown University. The founder of OTH Intelligence Group and a nonresident senior fellow with the Scowcroft Center for Strategy and Security at the Atlantic Council. “EYE TO EYE IN AI: Developing Artificial Intelligence for National Security and Defense” May. <https://www.atlanticcouncil.org/in-depth-research-reports/report/eye-to-eye-in-ai/> //barn

Engaging allies and partners: As noted at the outset of this paper, the war in Ukraine has reinforced the importance of allies and partners in enforcing geopolitical norms and standards. The same is likely to be true of the future of AI development and adoption. The DoD will benefit not only from collaboration across industry and the national security community, but also with allies and foreign partners to ensure establishment and promulgation of norms and standards that will enable trusted, responsible, and interoperable AI development and deployment.

#### Stopping zero-day loopholes and information analyzation are key to responding to Russian Information warfare in Ukraine

Charlie Greenbacker and Nic Acton 22, Head of Federal and Strategic Technology Programs at Snorkel AI. Federal Solutions Architect at Snorkel AI. “How AI can be used to rapidly respond to information warfare in the Russia-Ukraine conflict” February 28. <https://snorkel.ai/ai-response-to-information-warfare/> //barn

\*edited for ableist language\*

Information Warfare

The use of technology in the current conflict creates a daunting scale of impact. Russia is currently engaging in a three-front information offensive against Ukraine.

Disinformation: Over the past decade, Russia has developed and honed the largest and most comprehensive influence operation in human history. These capabilities are now used in a targeted, adversarial approach to reduce the morale of Ukrainian citizens, bolster Russian sympathizers in the Donbas region, and drum up support for the campaign amongst Russian citizens. Twitter, Facebook, and Telegram accounts can be generated automatically or bought by the thousands as disinformation signal generators.

Cyberwarfare: Russia is employing sophisticated cyberwarfare operations ranging from using malware to ~~cripple~~ \*incapacitate\* Ukrainian weapon systems to shutting down access to government and infrastructure websites. One cyber probe can scan an entire network of systems looking for a single unpatched entry point. Once found, these entry points can be exploited through a massive, growing list of known common vulnerabilities and exposures (CVEs) and currently unknown zero-day exploits.

Kinetic warfare: This past week, Russia has expanded into kinetic operations, entering the theater with almost 4x the military assets of Ukraine. These kinetic offensives use automated signal collection and AI-enabled signals intelligence (SIGINT) to guide precision weaponry and specialized army units towards high-value targets.

The concurrent use of these three strategies is not a secret. It is Russia’s published playbook.

How AI can help counter information warfare

Responding effectively to the deluge of attacks is not manageable by human analysts alone. Fortunately, state-of-the-art AI approaches can exponentially scale the work of analysts and experts combating adversary efforts, and deploying these approaches rapidly is more possible than ever.

AI can be used in many ways to respond quickly to the information warfare operations being waged against Ukraine. Examples include:

Disinformation: Use natural language processing (NLP) to automatically identify disinformation, then take immediate action by publishing factual responses and removing adversarial social media accounts.

Cybersecurity: Develop anomaly detection applications to scale analysts’ ability to monitor vast networks and rapidly respond to incidents.

Kinetic warfare: Use information extraction to analyze signals and adversary communications, identify high-value information, and use it to guide diplomacy and decision-making.

#### NATO collaboration over AI is the new front of war in Ukraine

Richard L. Hudson and Florin Zubașcu 22, Richard was the managing editor of the Wall Street Journal's European edition for six years, and a Journal reporter and editor for twenty-five years. “Science goes to war: western allies step up collaboration in military research” April 07. <https://sciencebusiness.net/news/science-goes-war-western-allies-step-collaboration-military-research> //barn

The war in Ukraine moved directly into the lab this week, with western governments announcing a series of new measures to coordinate their military research, including on quantum technologies and hypersonic missiles.

But the shift isn’t without controversy, as some European academics urged the EU to keep its civilian and defence research separate.

The military build-up took several steps, with NATO announcing a coordinated, multi-country research programme, and the US, Australia and UK setting plans for expanded quantum, hypersonic and other joint weapons research. It followed a NATO leaders’ meeting last autumn in which the strategy was set; but the scale and scope of the detailed measures announced this week were massive.

DIANA launch

Jens Stoltenberg, secretary general of NATO, announced this week that the UK and Estonia will host a joint military R&D programme involving research centres around the alliance. The Defence Innovation Accelerator for the North Atlantic (DIANA) is expected to strengthen transatlantic cooperation on defence technologies and procurement.

The innovation accelerator will cover projects in artificial intelligence, big data, quantum technologies, biotechnology, hypersonics and space. “The goal of DIANA is to support deep technologies companies that contribute to defence,” said Estonian defence minister Kalle Laanet.

In the UK, Imperial College London will be the host organisation, coordinating what the UK government called “deep tech test centres” for military technologies, and a “virtual marketplace” to connect start-ups with investors and procurers.

The project is part of a broader NATO initiative to boost military research cooperation, that will ultimately involve as many as 60 sites. On 6 April, Denmark’s DTU research organisation said it and partners had been chosen to set up a NATO testing centre in Copenhagen for quantum technologies. Further announcements on other sites to be included are expected in coming weeks.

#### Cyber-attacks escalate and trigger Article 5, triggering all-out war between nuclear states---Sanctions supercharge uniqueness because counterattacks are the only option left

Digital Watch Observatory (DWO) 22, The Digital Watch is an initiative of the Geneva Internet Platform, supported by the Swiss Confederation and the Republic and Canton of Geneva. “Ukraine conflict: Digital and cyber aspects” June. <https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects> //barn

The current political climate presents a high possibility for cyberattacks to get out of control and escalate beyond the conflict in Ukraine. Some countries have already expressed their concerns about possible cyberattacks targeting their national critical infrastructures. And there are several possible scenarios for escalations to occur in the near future.

Russia, in line with its aggressive decision to put its nuclear forces on high alert, might respond with devastating cyberattacks. On the other hand, NATO has already confirmed that a cyberattack against any of its members would trigger Article 5 of the NATO Charter, allowing NATO to strike back with all means available. In the past, the USA and its allies have primarily resorted to public attribution of attacks to Russia and, eventually, some sanctions against the individuals involved. With their portfolio of sanctions now almost completely deployed already, there is not much more that they could do to respond economically to such attacks – so counter cyberattacks are a possible option.

#### Ukraine risks international cyber conflict

Dan Sabbagh 22, Sabbagh is the Defence and Security editor for the guardian. “Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief” May 10. <https://www.theguardian.com/technology/2022/may/10/russian-hackers-targeting-opponents-of-ukraine-invasion-warns-gchq-chief> //barn

Russian hackers are seeking to target western countries supporting Ukraine in its efforts to resist Moscow’s invasion, the head of GCHQ has said.

Jeremy Fleming, the director of the British spy agency, said in a speech on Tuesday morning that while fears of a fully fledged online war between Russia and Ukraine had perhaps failed to materialise, there remained “plenty” of cyber activity as part of the conflict.

As well as affecting Ukraine directly, there had been “some spillover of activity affecting other countries”, Fleming said, and evidence that Russian actors were trying to escalate the conflict further afield.

“We’ve seen indications that Russia’s cyber operatives continue to look for targets in countries that oppose their actions,” the GCHQ chief said. “That’s why we have increased our efforts to ensure UK businesses and government urgently improve levels of cyber resilience.”

Fleming did not provide extra evidence, but last month, Britain’s National Cyber Security Agency, an arm of GCHQ, joined forces with its US counterpart, the Cybersecurity and Infrastructure Security Agency, in producing an advisory notice warning against a potential Russian escalation.

At the time they warned there was a risk some Russian criminal hackers “have recently publicly pledged support for the Russian government” and that they could be willing to engage “in retaliation for perceived cyber offensives against the Russian government or the Russian people”.

Russia has been accused of staging more than 200 cyber-attacks on Ukraine since launching its invasion on 24 February, according to an analysis from Microsoft, targeting government agencies and media companies with hacking attempts or destructive malware designed to disable systems.

Fleming said the UK, in conjunction with the US and other allies, was engaged in continuing “to support Ukraine in shoring up their cyber defences” – a recognition that the country is the frontline of what could yet spread into an international cyber conflict.

Last month, Ukraine said Russian hackers had tried to take out the country’s power grid, and came close to cutting off power for about 2 million people using a variant of the Industroyer malware. Although these attacks were aimed at Ukraine, there remains the risk that such malware could spread uncontrolled.

#### Ukraine is a flashpoint for US-Russia AI race, risking escalation

Brank Marijan 22, A senior researcher at Project Ploughshares, where Brank leads research on the military and security implication of emerging technologies. “Beyond Ukraine: AI and the Next US-Russia Confrontation” February 14. <https://www.cigionline.org/articles/beyond-ukraine-ai-and-the-next-us-russia-confrontation/> //barn

Two titans from the Cold War era seem set to go another round, this time over the prospect of Ukraine’s membership in the North Atlantic Treaty Organization (NATO), which the United States calls a sovereign Ukrainian decision and Russia opposes vehemently. Whatever the outcome of the current standoff, another confrontation between the United States and Russia that merits closer attention is brewing — one that may fundamentally reshape the US-Russia security relationship in the not-so-distant future.

Both states are heavily committed to the use of artificial intelligence (AI) in military systems and operations, including logistics, command and control, and intelligence collection and analysis, as well as to the development of more autonomous weapons. As tensions rise, these countries are likely to employ capabilities that are enhanced by AI and machine learning in cyberattacks and misinformation and disinformation campaigns. Rising political temperatures might well encourage fast-tracking of more autonomous military systems as each side seeks to gain the advantage.

The United States and Russia have already tested several autonomous systems. Russia has made important advances on autonomous tanks, while the United States has demonstrated a number of capabilities, including swarming munitions, which have the ability to destroy a surface vessel using a swarm of drones. At the moment, the United States is at the forefront of the development of autonomous systems and military AI applications. However, Russia has approached China to partner with it in building its AI readiness, and such a partnership could be a game changer.

One crucial concern is that the growing autonomy and use of AI in decision making in existing weapons platforms and in cyberspace will result in the deployment of immature systems; the result could be accidents that help to escalate conflict.

At the same time, both Russia and the United States have prevented progress on new international norms and agreements on the development and use of autonomous systems that could help to avoid dangerous situations. The United States and its allies are developing norms on responsible military uses of AI, but little dialogue with potential adversaries has taken place. And so, the competition between the great powers is allowed to grow unchecked.

Both Russia and the United States have prevented progress on new international norms and agreements on the development and use of autonomous systems that could help to avoid dangerous situations.

Understanding the Role of AI in Contemporary Conflicts

A key challenge is that AI itself is not a weapon but a range of functions and technologies. As Michael C. Horowitz has noted, AI can be defined as enabling technology: “AI is not a single widget, unlike a semiconductor or even a nuclear weapon.” In other words, AI is many technologies and techniques. Such an interpretation helps us to understand the range of current and potential uses of this technology in defence applications, including in cyberattacks and digital information warfare, as well as in more autonomous weapons systems.

The United States and other NATO members are already bolstering Ukrainian cyber defences in expectation of cyberattacks by Russia on Ukraine’s infrastructure, including its electrical grid, communication systems and government departments. Yet Russia could use AI to overwhelm Ukrainian systems in conjunction with misinformation and disinformation campaigns, some of which might involve manufactured or manipulated images or video, known as deepfakes.

While cyber and misinformation tactics are not new, AI and machine learning are offering novel ways to engage in them. And, while Western media and analysts focus on Russian cyber techniques, it is almost certainly true that the United States and other NATO members are also pursuing some of these same tactics against Russia.

Most states publicly agree that crossing a certain threshold of cyber activity, as in the targeting of critical infrastructure, could justifiably be perceived as akin to an actual physical attack. Still, it seems possible that some activities short of this threshold are taking place and contributing to the escalation of conflict. UN discussions on responsible behaviour in cyberspace have sought to build shared norms, but more work needs to be done for concrete rules to be established.

#### Cyber is the only scenario for escalation---Putin understands conventional attacks in NATO territory are a non-starter, only leaving the scenario of miscalculation and cyber warfare

Nadine El-bawab 22, A correspondent for ABC news. “NATO's Article 5 could pull the US and its allies further into the Russia-Ukraine conflict” March 01. <https://abcnews.go.com/International/natos-article-pull-us-allies-russia-ukraine-conflict/story?id=83108600> //barn

President Joe Biden repeatedly has said the United States will not be sending troops to fight Russia in Ukraine, but vowed that the U.S. would defend its NATO allies.

"As I made crystal clear, the United States will defend every inch of NATO territory with the full force of American power," he reiterated in an address Thursday.

The main goal of the North Atlantic Treaty Organization's founding in 1949 was to foster mutual assistance in response to the Soviet Union's expansion in Europe. A key component of the treaty, Article 5, covers "collective defense," which means that an attack on one ally is considered an attack on all allies.

Amid the current crisis, Article 5 could mandate a more direct response from the U.S. and other treaty members if Russian aggression escalates beyond Ukraine.

NATO announced last week it launched its response force, a deployment of about 40,000 troops to provide land, air and naval assistance across the alliance. This is the first time the force has been deployed for a "deterrence and defence role," a NATO spokesperson said.

Charles Kupchan, a senior fellow at the Council on Foreign Relations and professor of international affairs at Georgetown University, told ABC News it is possible Article 5 could be invoked while the U.S. and its allies are providing military aid to Ukraine.

“Let's say that Russia succeeds in toppling the government. And it then tries to occupy and pacify Ukraine. Assuming that the U.S. and its allies attempt to get arms to a Ukrainian resistance movement, there's a not insignificant risk that Russia might try to interdict that flow. And that whether by design or by accident, an artillery shell or a missile or a bomb could land in Poland or another NATO country,” Kupchan said.

“And then we're looking at the prospect of an attack on NATO territory and the potential trigger of the Article Five collective defense guarantee, which then raises the prospect of potential military conflict between NATO and Russia,” Kupchan said.

All participating countries agree to the form of solidarity outlined in the article, making it a key component of the alliance. While Ukraine is not a member of NATO, it borders Poland, Hungry, Slovakia and Romania, which are members.

Ukraine has been moving toward the West and away from Russia, attempting to join both NATO and the European Union. Kupchan said its geographical location could be strategic during this conflict

“In the current moment, Ukraine's border with four NATO countries affords it two important advantages,” Kupchan said. “One is refugees are able to seek asylum in NATO countries, and we're seeing hundreds of thousands of Ukrainians head west. And the other is that now that Ukraine's airspace is … dominated by Russia, the long border between Ukraine and NATO affords an opportunity to continue to funnel weapons and other sources of support to Ukraine."

The first time Article 5 was invoked was after the terrorist attacks of Sept. 11, 2001. The alliance had already identified terrorism as a risk affecting its security in 1999. In response to the attack, NATO engaged in the fight against terrorism, launching its first operations outside the Euro-Atlantic area to patrol the skies over the U.S.

In 2008, NATO appeared to open the door for Ukraine's membership saying it would become a member of the alliance, despite a lack of consensus between members, Kupchan said. NATO did not specify a pathway or timeframe for Ukraine to join the alliance.

“In 2008, the Bush administration wanted to proceed with what's called a Membership Action Plan for Ukraine and Georgia. And European partners were reluctant, in part because neither Ukraine nor Georgia was ready to join NATO and because of concern that NATO's enlargement to Georgia and Ukraine would be seen as provocative in Russia,” Kupchan said.

“Given the lack of consensus within NATO, the alliance agreed to issue a generic statement that Georgia and Ukraine would become NATO members, but didn’t specify a timeframe or a pathway,” Kupchan said.

Russian President Vladimir Putin linked the current crisis to Russia's NATO demands, including a guarantee that NATO will stop expanding to the East, in a video address days before Russia invaded Ukraine. Putin accused the U.S. and NATO of ignoring his demands and blamed the West for the Ukraine crisis.

"[Putin] has said explicitly that he wants to see NATO's military presence [reduced] in the eastern flank and that would include the three Baltic countries, Poland, Romania, Hungary, Slovakia, " Kupchan said. "He wants to see NATO pull its capability back."

"One of the tragic dimensions of this conflict is that the Russians knew full well, that Ukrainian membership in NATO was not under consideration. It was not on the table. And NATO governments were quite explicit about that. Nonetheless, Putin decided to invade the country," Kupchan said.

Its unlikely Putin would launch an attack on a NATO ally because he would be looking at a "full-scale war," he said.

"My guess is that he understands that this is a non-starter," Kupchan said.

### deterrance

#### AI detection and readiness key to deter conflict in Ukraine in Taiwan---also key to solve terror attacks

Colin Demarest 22, Reporter at C4ISRNET, where he covers military networks, cyber and IT. “McMaster says AI can help beat adversaries, overcome ‘critical challenges’” May 17. <https://www.c4isrnet.com/artificial-intelligence/2022/05/17/mcmaster-says-ai-can-help-beat-adversaries-overcome-critical-challenges/> //barn

The U.S. must “identify aggression early to deter it,” McMaster told attendees of the daylong event focused on autonomy, AI and the defense policy that underpins it. “This applies to our inability to deter conflict in Ukraine, but also the need to deter conflict in other areas, like Taiwan. And, of course, we have to be able to respond to it quickly and to maintain situational understanding, identify patterns of adversary and enemy activity, and perhaps more importantly, to anticipate pattern breaks.”

Specific applications of AI, McMaster said, include “early warning of hostile actions by enemies and adversaries who possess long-range missile and rocket capabilities,” such as Russia or China. The capability “also applies to North Korea and Iran,” he continued. “It applies to Houthi rebels in Yemen, to Hezbollah in southern Lebanon, or Hamas in Gaza.”

## AT: Centralization Bad

### Centralization Good

#### AI centralization improves administration in government programs and protects national security

David S. Rubenstein 20, Professor Rubenstein is James R. Ahrens Chair in Constitutional Law and Director of the [Robert J. Dole Center for Law and Government](https://www.washburnlaw.edu/practicalexperience/government/center/) at Washburn University School of Law. He teaches and writes in the areas of administrative law, constitutional law, artificial intelligence, legislation, jurisprudence, and federal contracting, “Acquiring Ethical AI,” Florida Law Review, Vol. 73, November 1 2020, http://www.floridalawreview.com/wp-content/uploads/2\_Rubenstein\_BOOK.pdf//RA

Ideally, AI can make government more efficient and effective across a wide range of functions: law enforcement, adjudication, rulemaking, national security, resource allocation, in-house management, delivery of public services, and beyond.115 Moreover, with proper design, AI systems can provide greater accuracy than human deciders alone.116 Further, AI systems may be more transparent and accountable than government agents, who might conceal or be unaware of their own cognitive biases.117

The centralization of AI decision-making may also promote greater consistency across cases, both in public-facing operations (such as adjudication and law enforcement) and inward-facing operations (such as personnel retention).118 What’s more, centralized AI decision-making can facilitate audits of external and internal government programs.119

The government’s adoption of AI technologies may also be fiscally responsible. By “automating repetitive tasks” and “augmenting” the capabilities of federal workers, taxpayer dollars can be saved or rerouted to better use.120 According to one rosy estimate, the government’s widespread adoption of AI could yield $500 billion in cost reductions over the next decade.121

Suffice to say, AI has the potential to augment, enable, and vastly improve government operations. Beyond better, however, the government’s rapid uptake of AI is arguably imperative “to protect [the nation’s] security, promote its prosperity, and safeguard the future of democracy.”122 That was a top-line message delivered by the National Security Commission on Artificial Intelligence (NSCAI) to the President and Congress in 2021.123

While this Article is principally focused on civilian and domestic contexts, the global “AI arms race” is quite relevant here. Foremost, the global competition exerts gravitational pull on the government’s entire AI trajectory. 124 More concretely, the race anchors the government’s ambition to “retain [America’s] innovation leadership”125—which depends mightily on the industry’s capacities and cooperation. Further, the U.S./China juxtaposition—and narratives around it—crystallize the need for AI innovation and ideation that reflects American values.126 As put by the NSCAI: If AI systems violate civil rights, or “have significant negative consequences, then leaders will not adopt them, operators will not use them, Congress will not fund them, and the American people will not support them.”127

#### [Centralization](https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4229/RAND_RR4229.pdf) is key to success and stability – decentralization of DOD AI will be destructive to the agency

DANIELLE C. Tarraf et al. 19, TARRAF, WILLIAM SHELTON, EDWARD PARKER, BRIEN ALKIRE, DIANA GEHLHAUS CAREW, JUSTIN GRANA, ALEXIS LEVEDAHL, JASMIN LÉVEILLÉ, JARED MONDSCHEIN, JAMES RYSEFF, ALI WYNE, DAN ELINOFF, EDWARD GEIST, BENJAMIN N. HARRIS, ERIC HUI, CEDRIC KENNEY, SYDNE NEWBERRY, CHANDLER SACHS, PETER SCHIRMER, DANIELLE SCHLANG, VICTORIA SMITH, ABBIE TINGSTAD, PADMAJA VEDULA, KRISTIN WARREN, Danielle Tarraf is a publisher at Rand Corporation, “The Department of Defense Posture for Artificial Intelligence,” June 2019, https://www.rand.org/content/dam/rand/pubs/research\_reports/RR4200/RR4229/RAND\_RR4229.pdf//RA

The JAIC lacks visibility. The issue of visibility is subtle. The JAIC has been designated, in the summary of the DoD AI strategy, as the focal point for carrying out DoD’s strategy, and is expected to attract and cultivate a world-class AI team. This designation and role presume a certain degree of visibility both within DoD and outside it. This visibility was lacking based on our interviews. Overall, we noted a lack of clarity among our interviewees on the JAIC’s mandate, roles, and activities. We also noted a lack of clarity around how it fits within the broader DoD ecosystem and how it connects to the services and their efforts. That was true of both DoD interviewees and our industry interviewees who had heard of the JAIC (see section “Organization: At the OSD Level” in Appendix B and section “Thoughts Across Industry: On the JAIC” in Appendix C). In addition to the lack of clarity about the JAIC’s current mandate and roles, there were many perspectives about the desired or ideal role for the JAIC as DoD embraces and scales AI. These perspectives ranged from the JAIC as a central repository of information and best practices, to the JAIC as a center of excellence that focuses on discrete tasks (e.g., building the JCF, formalizing standards for VVT&E), to the JAIC’s potential elevation to a field agency or other entity with a direct reporting line to either the Secretary or DSD.

We do not believe this lack of clarity to be simply a question of messaging. More fundamentally, it points to a lack of clarity about the raison d’être of the JAIC and how the specific roles it has been assigned support that. The confusion might not be entirely on the part of the audience. DoD needs to have a clearer view of what it wants the JAIC to be and how DoD can help ensure the success of JAIC’s mission, and therefore DoD’s vision.

The DIB’s Technologies and Capabilities Recommendation  5, cited earlier in this chapter, proposed establishing a centralized, focused, and well-resourced organization to propel applied research in AI and ML forward. The insights gathered from our industry interviews (see section “Industry: Organization” in Appendix C) lead us to believe there is indeed value in, if not strict necessity for, a centralized organization. This organization would have a mandate that goes beyond applied research and would be supported at the highest levels with long-term funding commitments to institute organizational change and scale AI across DoD. One of our industry interviewees noted that centralization at onset was key to their organization’s success, and premature decentralization of effort likely would have been detrimental (see section “Industry: Organization” in Appendix C).7

Based on the premises that (1) the JAIC is the focal point of DoD AI activity; (2) it fulfills the need for a centralized, well-resourced organization to scale AI and its impact across DoD (see above); (3) it will continue in that role for several years because of the expected timeline for AI deployment at scale across enterprise, mission-support, and operational AI; and (4) it needs to be able carry out all the roles it has been tasked with in the current strategy and establishing memo, we identified friction points that we discuss in the following paragraphs.

### Perm

#### **Only centralization and decentralization in accordance with each other solve – the perm solves best**

Matthew R. Voke 19, Matthew R. Voke is a major at USAF, “Artificial Intelligence for Command and Control of Air Power,” Air Command and Staff College, June 2019, https://media.defense.gov/2019/Nov/27/2002218265/-1/-1/0/WF\_72\_VOKE\_%20ARTIFICIAL\_INTELLIGENCE\_FOR\_COMMAND\_AND\_CONTROL\_OF\_AIR\_POWER.PDF//RA

US doctrine prescribes the conduct of joint air operations using the principle of centralized control and decentralized execution.22 An oversimplified synopsis driving this tenet of airpower is that centralization of control enables the 5 senior echelon commanders to control, mass, and lead forces effectively; decentralization of execution allows forces to seize the initiative, respond to uncertain and changing environments, and fosters flexibility in lower echelons.

Technological developments frequently shift the equilibrium of this tenet of airpower. Robust communications connectivity has increased the shared operations picture at all levels, but it has also enabled senior leadership involvement in the finest details of employment.23 This duality has created inherent tension between the imperatives of political control and those of efficient mission accomplishment that leaders must understand.24 Although centralized control and execution are possible in many situations, a conscious effort to delegate execution authority appropriately will ensure the maintenance of US airpower agility.

The balance of centralization and decentralization can shift between and during conflicts, and leaders must strive to increase what some call “agility” in airpower employment. The Air Force Future Operating Concept defines agility as the ability to react rapidly to situations. Agility is a combination of one’s flexibility, speed, coordination, balance, and strength.25 Decentralization generally favors flexibility and speed, while centralization generally favors coordination and strength. One’s understanding of agility might imply physical capability, but agility also includes a cognitive capability to react to a dynamic opponent, moving target, or shifting environment.26 The power of AI employment in airpower C2 lies in the cognitive speed and strength it can bring synergistically toward the goal of agility.

## AT: Non-Democratic Country PIC

### 2ac – ukraine thumps

#### The war in Ukraine guarantees NATO has bigger fish to fry

Edward **Lucas, 6-7**-2022, "NATO Is Out of Shape and Out of Date," Foreign Policy, Edward Lucas is a nonresident fellow at the Center for European Policy Analysis, a Liberal Democratic candidate for the British Parliament, a former senior editor at The Economist, and the author, most recently, of Cyberphobia: Identity, Trust, Security and the Internet. https://foreignpolicy.com/2022/06/07/nato-ukraine-russia-war-alliance-reform-geopolitics-military/, accessed 6-28-2022//cpd (EDITED FOR ABELIST LANGUGE)

Is NATO ~~brain-dead~~ [OBSOLOTE] or back in business? Less than three years ago, French President Emmanuel Macron famously diagnosed “the ~~brain death~~ of NATO.” Rhetoric aside, his point was fair at the time: Europe’s dearth of strategic thinking combined with the unpredictability of U.S. policy under then-President Donald Trump spelled serious trouble for the Cold War-era alliance.

Now, all talk is of NATO’s revival and resurgence. Russia’s war on Ukraine has given an urgent new relevance to the bloc’s core mission of territorial defense. NATO members appear to have found a new unity of purpose, supplying Ukraine with weapons, reassessing the threat from Russia, hiking defense budgets, and bolstering the security of the alliance’s eastern frontier. But the “honeymoon,” in the words of Lithuanian Foreign Minister Gabrielius Landsbergis, was brief. As the war drags on, strains are showing, and the alliance is still shaky.

It’s true that NATO has come a long way. Only 14 years ago, the alliance’s top-secret threat assessment body, MC 161, was explicitly prohibited by its political masters from even considering any military danger from Russia in its scenarios. The pressure came not only from notorious Russia-huggers such as Germany but also from the United States, which was eager to keep east-west ties friendly. The Kremlin, the conventional wisdom insisted, was a partner, not an enemy. As a result, NATO’s most vulnerable members—Poland and the Baltic states of Estonia, Latvia, and Lithuania—remained second-class allies. They were in the bloc, but only on paper. There were no significant outside forces on their territory, and the alliance expressly refrained from making contingency plans to reinforce or even defend them in the event of attack. Poland demanded such plans and was told that they could be drawn up to defend the country against an attack by Belarus—but not by Russia.

Since Russia’s first attack on Ukraine in 2014, NATO plans and deployments have become more serious. There are 1,000-strong tripwire forces in the three Baltic states and a larger U.S. force in Poland. Since the start of the invasion in February, that presence has increased sharply. Moreover, two of the most advanced smaller military powers in Europe, Finland and Sweden, are banging on the alliance’s door. Assuming objections from Turkey can been smoothed out, they will be members by year’s end. That will fundamentally change the military geography of northeastern Europe.

Still more important is the stiffening of spines among the members. Trump’s much publicized distaste for NATO was based, in part, on the European members’ chronic underspending. At one point, the exasperated U.S. leader even tried to present a bill to his German counterpart, Chancellor Angela Merkel. Now, defense spending is rising across the alliance. That makes NATO an easier sell in Washington, especially as the case for U.S. engagement in European security is bolstered by the war in Ukraine.

Scholzen is a German neologism for “dither,” while makronic in Polish (and its equivalent in Ukrainian) can be roughly translated as “vacuous grandstanding while doing nothing.”

Germany, the most notorious laggard, is suddenly splurging money on its decrepit armed forces—tanks that can’t trundle, ships that can’t go to sea, and soldiers who exercise with broomsticks instead of guns. It has agreed to meet NATO’s defense spending benchmark of 2 percent of GDP, set in 2006 and largely ignored thereafter. The latest country to announce a big hike in defense spending is Spain, currently lagging at barely 1 percent of GDP. The prime minister announced that this will double by 2024. That sets the scene nicely for the NATO summit in the Spanish capital later this month.

Yet look a little more closely, and the picture is far less rosy. Notwithstanding its apparent unity of purpose since the start of Russia’s war, NATO looks out of shape and out of date. In the run-up to their summit, the allies have been furiously haggling over the language in their new strategic concept, which will frame the alliance’s mission for the coming years and will be unveiled in Madrid. What will it say about Russia? About China? What sacrifices and risks are the member states really willing to accept? Are they willing to pool sovereignty in order to streamline decision-making?

Nothing in recent weeks suggests that these questions will get clear answers. For starters, the 30-strong alliance is unwieldy. In military terms, only a handful of members matter—above all, the United States—but in political terms, even little Luxembourg and Iceland get a voice. Worse, the political divides are huge. Turkey under President Recep Tayyip Erdogan is a semi-authoritarian state that flirts with Russia and fumes at what it considers European meddling over human rights. Hungary under Prime Minister Viktor Orban is taking a different but downward path, fusing wealth and power into a new system of control at home and undermining U.S. and European attempts to put pressure on Russia and China. Macron’s relentless posturing and German Chancellor Olaf Scholz’s foot-dragging create constant obstacles and distractions. The two leader’s weaknesses, on glorious display since the start of the war, have already enriched the language: Scholzen is a German neologism for “dither,” while makronic in Polish (and its equivalent in Ukrainian) can be roughly translated as “vacuous grandstanding while doing nothing.”

Macron and Scholz corrode decision-making with their foibles and thus place a big question mark over the alliance’s credibility and cohesion. Any threat or provocation from Russia is unlikely to be clear or conveniently timed. More likely it will be something deliberately ambiguous, such as a Russian drone that “accidentally” strays onto the territory of a front-line state and hits a target. Some countries would favor a tough response. Others would fear escalation and want dialogue. Still others would take the ambiguity as a convenient excuse to do nothing. Would the 30—soon to be 32—national representatives in the North Atlantic Council, the alliance’s deliberative body, really make a speedy and tough decision on how to react? More likely, some of them would plead for delay, diplomacy, and compromise. Those actually facing the possibility of attack would be far more hawkish, preferring a sharp military confrontation to even the smallest Russian victory. “Not one inch, not one soul,” a senior military figure from one of the Baltic states, speaking anonymously, told me. “We have seen what they did in Ukraine.”

The political weaknesses are matched by military ones. By far the most important country in the alliance is the United States. The U.S. security guarantee to Europe—with its threat of devastating conventional and, if necessary, nuclear response to any attack—is the cornerstone of the alliance. “All for one and one for all” sounds fine, but nobody in the Kremlin will tremble at the thought of Spanish, Dutch, or Canadian displeasure. Yet the result of this is a colossal dependence on U.S. capabilities, ranging from ammunition and spare parts (of which European countries’ stockpiles are notoriously skinny) to military transports that move forces quickly and efficiently over long distances. Even if Europe’s new defense spending plans materialize, they will not change the fact that only U.S. armed forces can move with the scale and speed necessary to defend territory from a country like Russia.

Conversely, the countries that most need defending—Estonia, Latvia, and Lithuania—are the least able to bear the burden themselves. They need advanced weapons, particularly for air and missile defense, that they cannot afford themselves. The thin neck of land along the Polish-Lithuanian border, the so-called Suwalki Gap, is particularly vulnerable to attack from Russia’s militarized Kaliningrad exclave and Belarus, from which Russia attacked Ukraine. Poland and Lithuania both want a big U.S. military presence—either a permanent base or a persistent rotation of forces—to safeguard this strategic chokepoint.

Yet NATO command structures and planning do not fully reflect the imbalance of forces between the United States and Europe. They rely on the fiction that the European allies are more or less equal partners. Even military lightweights need to have important-sounding jobs and installations, making the North Atlantic Council the military version of a parliament dividing out the pork.

The resulting command structure is like a tangled pile of spaghetti. In the Baltic region alone, NATO has several multinational headquarters, one divisional headquarters split between Latvia and Denmark, another divisional headquarters in Poland, and a corps headquarters at a different location in Poland. Overall responsibility for the defense of Europe is divided between three Joint Forces Command headquarters in Naples, Italy; Brunssum, the Netherlands; and Norfolk, Virginia. But the top U.S. military commander in Europe, Air Force Gen. Tod Wolters, is based at Supreme Headquarters Allied Powers Europe in Mons, Belgium. A maritime strategy for the Baltic Sea region has yet to be decided—which is just as well, because NATO has yet to create a naval headquarters for the region. Nor has the alliance drawn up real military plans for the reinforcement and defense of its northeastern members, let alone decided who would actually provide the forces and equipment in order to make them credible. Military mobility is meant to be the responsibility of Joint Support and Enabling Command, headquartered in Ulm, Germany, and originally set up as part of the European Union’s own defense policy.

### 2ac – cooperation inev

#### The is confronting the Greek-Turkish conflict now, but exclusion of Turkey in NATO operations risks sending the wrong signal

Seth **Cropsey**, **6-23**-2022, "Diversionary war: Turkey’s actions against Greece are a growing threat to NATO," Hill, https://thehill.com/opinion/national-security/3534155-diversionary-war-turkeys-actions-against-greece-are-a-growing-threat-to-nato/, accessed 6-28-2022//cpd

Turkish obstructionism against Swedish and Finnish NATO membership, its limited offensive in Iraq, and its prospective offensive in Syria have grabbed international attention. But more significant is Turkey’s growing diplomatic tension with Greece, an ever-festering lesion that threatens to burst.

Considering Turkey’s domestic situation and Russia’s invasion of Ukraine, the United States must be wary. Turkish President Recip Tayyip Erdogan could capitalize on international distraction and wage a diversionary war to boost his popularity, a conflict that would disrupt NATO’s cohesion and threaten the alliance.

Washington should act now to resolve the current incarnation of this long-standing Mediterranean dispute.

Recep Tayyip Erdogan has dominated Turkish politics since 2001, when his AKP party first won a two-thirds parliamentary majority. Although Erdogan was banned from Turkish politics for anti-secular incitement, his prime ministerial — and, later, presidential — predecessor, Abdullah Gül, until the mid-2010s at least, was functionally a stand-in for him. Erdogan may have restricted his Islamist proclivities and international assertiveness until he consolidated power in 2014-2016. However, Turkey’s break with the United States over the latter’s invasion of Iraq, and Turkey’s growing hostility towards Israel, indicated a deeper rift between Washington and Ankara. Erdogan consistently sought a greater regional role; through diplomatic pressure against Israel culminating with the Gaza Flotilla — a bald-faced attempt to prompt a confrontation with Israel — Erdogan hoped to position himself as the spiritual leader of the Islamic world.

The Arab Spring, however, transformed the regional balance. No power could pretend that the “Palestine Question” still defined regional politics. The Libyan and Syrian civil wars, and the subsequent rise of ISIS, thrust Islamism to the fore once again, while Iranian expansion in Iraq, Syria and Lebanon demonstrated the relevance of traditional coalition competition, rather than religious rivalry.

Turkey’s response has been to sharpen its shift away from the United States by alternating between Russophilic and Russophobic policies.

The Levantine maelstrom that began in Syria and exploded in Iraq stoked Turkish fears of Kurdish revanchism. Even before that, Russian presence in Syria prompted Turkey to pursue a more aggressive policy, supporting Islamist elements in the Syrian opposition and destroying a Russian Su-24 that briefly violated Turkish airspace. Two years later, Turkey agreed to purchase S-400 anti-air systems from Russia that, in 2019, prompted its ejection from the West’s F-35 fighter-jet program and U.S. sanctions.

More generally, Turkey asserted itself militarily since 2016, intervening directly in Syria and Libya. In the latter conflict, Turkey aligned with the Tripoli-based Government of National Accord, opposing the Tobruk-based French-, Russian-, Emirati- and Egyptian-supported House of Representatives. Although fighting there has subsided, tensions may again explode — and by striking a territorial deal in Libya, Turkey can lay claims to the Eastern Mediterranean’s natural gas deposits, threatening Israel, Egypt and Greece.

Turkish actions during the Ukraine war have indicated Ankara’s desire to return to the Western fold. Initially, Turkey refrained from engaging, likely seeking to determine if Ukraine would collapse within days. However, three days into the war, when it became apparent Ukraine would resist, Turkey closed the Bosphorus Straits to Russia; Russian Black Sea Fleet warships in the Levantine Basin can still return to their home port in Sevastopol, but their inability to sortie from Sevastopol into the Mediterranean will disrupt Russian outer naval defenses in the long-term.

Turkey also attempted to position itself as a mediator between Kyiv and Moscow, and it spearheaded a half-hearted attempt (albeit with great public fanfare) to ensure grain exports from Ukraine.

Yet, Turkey’s resistance to Swedish and Finnish NATO memberships is a ploy to extract concessions from Washington: If the Biden administration reinstates Turkey in the F-35 program and approves F-16 sales, Erdogan likely will relent.

Buying Turkish acquiescence is no way to ensure a long-term strategic partnership, however. Indeed, Erdogan is laying the groundwork for another Greco-Turkish confrontation.

The focal point, once again, is Cyprus. Greece and Cyprus are linked by ethno-linguistic ties, political history and strategic interest. If Crete “caps” the Aegean, Cyprus provides Greece a pressure point against any Anatolian or Near Eastern power that would threaten it. Greece maintains a small military force in Cyprus, is a supplier to Cyprus’ small National Guard, and is a crucial Cypriot trading partner. However, in 1974, Turkey invaded Cyprus, capturing a third of the island and collapsing the Greek military junta that had organized a coup in Cyprus earlier that year. Turkey has not annexed Cyprus outright, instead establishing a satellite state on the island’s north that only Ankara recognizes. The current situation is tenable, although Turkey has used Northern Cyprus to tacitly extend its presence in the Levantine Basin.

Turkey’s agreement with Libya solidified its claims to the Eastern Mediterranean’s petrochemicals. With the Libyan civil war’s apparent conclusion, and Turkey’s desire to return to the Western camp, Erdogan might be expected to refrain from spoiling Greco-Turkish relations with moves in Cyprus or elsewhere — but he has done the opposite. Turkey has struck a major economic deal with Northern Cyprus that would increase Ankara’s direct leverage over the statelet; it would list Ercan airport, Northern Cyprus’s international aerial hub, as a domestic destination on Turkish flights. Cypriot authorities fear this is the first step towards outright annexation, which would shatter a UN-brokered ceasefire and undoubtedly prompt a Greek military response. Erdogan has also leveled threats over Greece’s alleged militarization of Aegean islands, despite Greece’s long-standing military presence in the Aegean.

In turn, an escalating economic crisis is ravaging Turkey. Food and energy supply disruptions have sharpened inflationary pressures with which Turkey has grappled since 2017. Erdogan’s refusal to increase interest rates and tighten the money supply is an advanced form of macro-economic foolishness; in 2021, the Turkish lira’s value

was slashed by half. Yet inflation remains at 60-plus percent and is likely to climb.

Erdogan’s AKP lost ground in nearly all major cities in the 2019 local elections. As the 2023 parliamentary and presidential elections approach, Erdogan may seek to distract domestic attention with a major foreign policy crisis, such as a confrontation with Greece.

The United States should ensure that this crisis does not stress NATO. Russia will employ every tool at its disposal to force a confrontation between Greece and Turkey, including hybrid provocations, diplomatic overtures, naval exercises and perhaps even false flags.

Preventing a crisis requires three steps, one military, two diplomatic.

First, the United States ought to increase its naval presence in the Eastern Mediterranean. Ideally, it would sustain a consistent carrier deployment to the Levantine Basin, as it did during the Cold War and has done since Russian designs against Ukraine neared their boiling point. The very presence of a U.S. carrier, with the combat power it provides, may be sufficient to deter Turkish escalation and demonstrate to Ankara that a diversionary crisis will only trigger more stresses for Erdogan’s regime. Second, the United States should convene a series of bilateral Turkish-Greek summits, similar to the “shuttle diplomacy” it practiced in the 1970s between Israel and its Arab adversaries, to coordinate policy with Northern Cyprus and the Cypriot Republic. At minimum, pinning Turkey in substantive dialogue will slow an escalation cycle. At best, the U.S., through skillful balancing, can address Turkish diplomatic demands and settle issues more generally. The next financial hammer to fall: Public pension funds Victory in Ukraine could mean a stalemate Third, the United States should prioritize reintegrating Turkey into NATO. This should involve both the sale of F-35s and F-16s with the caveat that Turkey must support U.S. activity in the Black Sea. Turkey should receive a reward for good behavior. But it should also offer something in return — for example, decreasing tensions on Cyprus or allowing Western ships to enter the Black Sea to clear Russian mines and escort merchant ships carrying Ukrainian grain to global ports.

As the Ukraine War drags on, the greatest threat to Western objectives will not be Russian military capabilities but divisions within NATO. A Greco-Turkish confrontation would threaten to upend the Atlantic Alliance at precisely the wrong time. It must be prevented.

### 2ac – turkey k2 nato

#### Black Sea DA- Turkey inclusion on NATO relations is key to future engagements in the Black Sea

Rachel **Ellenhuss** 12-2-20**19**, "Turkey and NATO: A Relationship Worth Saving," Rachel Ellehuus is deputy director and senior fellow with the Europe Program at the Center for Strategic and International Studies in Washington, D.C., https://www.csis.org/analysis/turkey-and-nato-relationship-worth-saving, accessed 6-25-2022//cpd

Yet these foundational factors remain valid: Turkey’s geopolitical position at the crossroads of Europe, Asia, and Africa still provides NATO with needed political and operational reach, and Turkey continues to benefit from the collective military power of NATO. With the relationship close to (if not at) its nadir, Turkey and NATO, with the support of the EU, need to take active measures to anchor it for the future, while avoiding steps that could destroy the relationship entirely.

Active measures

Assuming that Turkey is in fact interested in rebuilding the relationship with its NATO allies, there are several active measures NATO and Turkey can take now to create a foothold for the future. The key is to focus on areas of mutual interest where NATO involvement is critical to Turkish strategic interests and where Turkey has a unique role to play in NATO.

The first of these is the Black Sea, where Turkey, as well as fellow NATO Black Sea littoral states Romania and Bulgaria, are trying to balance an increasing Russian military presence. While previously resistant to a greater NATO role in the Black Sea for fear it would dilute its own influence in the region, Turkey now sees the dangers of leaving Russian influence and presence in Black Sea unchecked. With its illegal annexation of Crimea in 2014 and entry into the Syrian civil war in 2015, Russia has significantly increased its presence and combat capabilities in both the Black Sea and Eastern Mediterranean.

NATO now faces an anti-access/area denial (A2/AD) bubble that restricts allies’ freedom of maneuver in the Black Sea, with Russia capable of attacking from both land and sea. To effectively counter this, NATO should establish a more continuous presence in the Black Sea, revive the idea of a permanent NATO maritime fleet in the Black Sea, and consider basing more counter-A2/AD capabilities in Turkey and Romania. Importantly, Turkey holds unique power to control access to the Black Sea thanks to the 1936 Montreux Convention, which governs naval passage through the Turkish Straits, limiting the number of foreign vessels that can enter the Black Sea via the Straits and how long these vessels can stay. This access is important to both Russia and NATO. Whereas Turkey has proven to be an impartial and reliable enforcer of the treaty, Russia has pushed the boundaries of Montreux repeatedly since the Russo-Georgian War in 2008 and, more recently, impeded the course of NATO vessels that have entered and departed the Black Sea in compliance with the treaty. More behavior along these lines, or a Russian attempt to leverage its new, closer relationship with Turkey to secure more favorable access to the Black Sea, would likely increase Turkey’s unease and lead it to rely more on NATO as a counterbalance.

#### **! to Russia getting black sea**

### 2ac – a2 – sweden/finland

#### Ongoing negotiations solve Swedish/Finnish conflit with Turkey

**Reuters**, 6-1-20**22**, "Finland and Sweden say will continue NATO talks with Turkey," https://www.reuters.com/world/europe/finland-says-nato-talks-with-turkey-will-continue-2022-06-01/, accessed 6-25-2022//cpd

The Nordic neighbours applied to join NATO last month in response to Russia's invasion of Ukraine, but they have faced resistance from Turkey, which accuses them of being safe havens for Kurdish militants and wants them to scrap arms export bans. read more

"Together with Sweden, we will do our homework and prepare for the questions Turkey has," Finnish Foreign Minister Pekka Haavisto told reporters in Helsinki, commenting on talks that took place in Ankara last week.

NATO Secretary-General Jens Stoltenberg said during a visit to Washington that he would convene senior officials from Finland, Sweden and Turkey in Brussels in the coming days to discuss the issue.

U.S. Secretary of State Antony Blinken, after meeting Stoltenberg, said NATO members' security concerns should be taken into consideration, but said he was confident the accession process for Finland and Sweden would move forward. read more

A bid to join NATO requires unanimous backing from the alliance's current 30 member states.

Speaking at an event in Stockholm, Swedish Prime Minister Magdalena Andersson said she expected constructive meetings with Turkey to take place in the near future.

"Our responses to demands and also questions from Turkey we will take up directly with Turkey and also sort out any issues and misunderstandings that there might be," she said. read more

Turkey has accused Finland and Sweden of harbouring people linked to groups it deems terrorist organisations, including the Kurdistan Workers Party (PKK), but Haavisto said the PKK was already considered a terrorist group by all EU members, including Finland.

Haavisto gave no timeline for the ongoing talks with Ankara, but struck an optimistic note.

"Perhaps such a thought still exists that at the Madrid summit, NATO could have something positive to tell about expansion," he said, referring to a meeting of the alliance due to be held in Spain at the end of this month.