# AI

## Funding

### 1NC --- Private

#### High risk/high reward investments create necessary innovation – only a public/private partnership can create this

Bipartisan Center 20 [The Bipartisan Policy Center is a Washington, DC-based think tank that actively fosters bipartisanship by combining the best ideas from both parties to promote health, security, and opportunity for all Americans. Our policy solutions are the product of informed deliberations by former elected and appointed officials, business and labor leaders, and academics and advocates who represent both sides of the political spectrum. BPC prioritizes one thing above all else: getting things done., "Cementing American Artificial Intelligence Leadership: AI Research & Development", Bipartisan Policy Center, https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2020/08/BPC\_RD-AI-Paper\_RV5.pdf] Blitz

Lead in Research & Development Greater investments in artificial intelligence research and development are essential to maintaining American leadership in AI. Throughout the 20th century, the federal government played a critical role in fueling technological innovation by funding pivotal basic research. Government funding was essential to developing the transistor, GPS, and the internet—inventions that transformed the world economy. Yet over the past several decades, federal government spending on R&D as a percentage of GDP declined from about 1.2% in 1976 to around 0.7% in 2018.1 This is a worrisome trend as the federal government remains the main funder of basic research. Government support again could be pivotal both in fostering new AI breakthroughs and ensuring that the U.S. government has access to those breakthroughs. Beyond AI, overall R&D spending trends are troubling. Other countries are outpacing the United States with faster growth of their national R&D budgets. Total U.S. national (public and private) R&D expenditures as a share of GDP have been mostly stagnant since 1996. China quadrupled its R&D expenses as a share of GDP over the same time frame, and countries like Israel and Cementing American Artificial Intelligence Leadership: AI Research & Development AUGUST 2020 2 South Korea also significantly ramped up spending.2 As a result, the U.S. share of global R&D has declined over the past several decades, falling from 69% in 1960 to 28% in 2016. From 2000 to 2015, the United States accounted for 19% of global R&D growth, while China accounted for 31%.3 China was on track to top the United States in total R&D investments (in purchasing power parityadjusted dollars) as soon as 2019.4 R&D is a key driver of long-term economic growth. According to a report from BPC’s American Energy Innovation Council titled Energy Innovation Fueling America’s Economic Engine:5 TECHNOLOGICAL INNOVATION CAN IMPROVE PRODUCTIVIT Y ACROSS INDUSTRIES AND CRE ATE ENTIRELY NEW ONES. THIS IS ONE AMONG MANY RE ASONS WHY ECONOMISTS AGREE THAT INNOVATION IS A DRIVER OF LONG -TERM ECONOMIC GROW TH AND STABILIT Y—AND WHY AT LE AST 50 PERCENT OF U.S. ANNUAL GDP GROW TH CAN BE TRACED TO INCREASES IN INNOVATION. The Bipartisan Policy Center (BPC) and the Center for New American Security (CNAS), in consultation with Reps. Will Hurd (R-TX) and Robin Kelly (D-IL), have worked with government officials, industry representatives, civil society advocates, and academics to better understand the country’s major AI related R&D needs. This paper hopes to shed more clarity on these challenges and provide actionable policy recommendations, to help guide a U.S. national strategy for AI. BPC’s effort is primarily designed to complement the work done by the Obama and Trump administrations, including President Barack Obama’s 2016 National Artificial Intelligence Research and Development Strategic Plan6 and President Donald Trump’s 2019 update, Trump’s Executive Order 13859, announcing the American AI Initiative, 7 and the Office of Management and Budget’s subsequent Guidance for Regulation of Artificial Intelligence Applications. 8 The effort is also designed to further advance work done by Kelly and Hurd in their 2018 Oversight and Government Reform Committee (Information Technology Subcommittee) white paper Rise of the Machines: Artificial Intelligence and its Growing Impact on U.S. Policy9 and the CNAS report The American AI Century: A Blueprint for Action. Our goal through this effort is to provide the legislative branch with actions it can take to advance AI building on the work being done by the Obama and Trump administrations. 3 II. Key Principles 1. Overall federal AI R&D spending needs to increase significantly 2. The country needs to expand and diversify its computing capacity 3. The federal government plays a key role in incentivizing private sector R&D 4. There needs to be international cooperation to advance AI research and development 5. The federal government would benefit from opening up avenues for private talent 6. AI standards and measurement are essential to fostering AI technologies that are safe, secure, reliable, and comport with U.S. norms and values 4 III. Overview The private sector, academia, and the government have a long history of collaborating to advance technological innovation. Academia, often through support of federally funded grants, historically has conducted much of the basic research that has enabled the private sector to advance applied research and commercialize technologies. This partnership, however, is being strained by recent innovations in machine learning whose advancement relies on large datasets and compute resources that are increasingly unavailable to academic researchers. To ensure the United States is maximizing its R&D potential and to ensure the entire R&D cycle from basic research to commercialization is fully utilized, the partnership of government, academia, and the private sector must be strengthened to ensure each has adequate access to the resources they need while protecting intellectual property rights and data privacy. This includes standardizing and making current and future government datasets more readily available to the private sector and academia to facilitate training of machine learning models.10 Under the OPEN Government Data Act of 2019, federal agencies are required by statute to make available government datasets in standardized, machine-readable formats.11 Doing so will help to address data scarcity problems, especially for entities with significant resource constraints such as startups or some university researchers, by expanding the number of open-source high-quality datasets and increasing access to compute resources.12 5 IV. Key Takeaways Overall AI R&D spending needs to increase significantly The U.S. government remains the largest funder of basic research in the United States. As during the 1960s and 1970s, government support again could be pivotal today both in fostering new breakthroughs and ensuring that the U.S. government has access to them. The federal government should prioritize high-risk/high-reward basic science research—areas where private industry has little incentive to invest but that holds tremendous potential for valuable new knowledge. Breakthroughs in software, such as novel AI techniques that address the limitation of existing AI methods, and hardware, such as nextgeneration semiconductor technologies and superconducting artificial neurons, could be game changers that provide the United States with a continuing technological edge. Advances in AI can also further R&D of other fields because of its broad, interdisciplinary nature, while breakthroughs in areas like neuroscience can greatly advance AI development. Unclassified federal government spending on defense AI R&D in fiscal year 2020 will be about $4 billion, according to a Bloomberg analysis from March 2019.13 In September 2019, the White House announced an FY2020 nondefense AI R&D budget request of nearly $1 billion.14 In contrast, the level of Chinese government spending on AI R&D is not clear. Complete annualized figures for Chinese government spending are not publicly available. Instead, only announcements of planned, multi-year spending offer a window into the scale of overall government R&D spending at the national, provincial, and local levels.15 For instance, two Chinese cities alone announced the creation of RMB 100 billion (approximately $15 billion) multi-year AI development funds while Beijing unveiled plans for a $2 billion AI research park in 2018.16 The United States enjoys robust private sector R&D funding. Precise figures are hard to discern because companies typically do not divulge details for R&D expenditures in their financial statements and privately-owned firms do not have such reporting requirements. That said, looking at overall R&D expenditures by major AI-intensive companies gives a sense of the scale of private investments in AI R&D. The combined 2018 R&D expenditures by U.S. firms Alphabet, IBM, Facebook, Microsoft, and Amazon was $80.5 billion.17 China’s tech giants also report significant R&D investments, although they are considerably smaller than those of their U.S. counterparts. Leading Chinese AI firms Alibaba, Baidu, and Tencent collectively spent $9.1 billion on R&D in 2018.18 These firms are also major investors in Chinese AI startups.19 6 In April 2020, the National Security Commission on Artificial Intelligence (NSCAI) published its first quarter recommendations, calling for an immediate doubling of non-DOD AI R&D funding to $2 billion. NSCAI emphasized the importance of funding basic research and investing in new microelectronics technologies. This echoes the White House AI R&D budget request for FY2021-22.20 Recommendation #1: Congress and the White House should adopt the NSCAI and White House recommendations to double AI R&D spending immediately, and further commit to boosting total yearly federal AI R&D spending to $25 billion by FY2025. Spending at this level is realistic and doable: $25 billion is equal to about 19% of total federal R&D spending in the FY2020 budget. Congress should concurrently raise total federal R&D spending to 1.2% of GDP to achieve an overall boost of total public and private R&D spending to 4% of GDP. Recommendation #2: Congress should ensure R&D includes funding to address shortcomings of current AI methods with novel fundamental approaches: prevalent deep learning systems in use today typically require large amounts of training data and computing resources that are often not available to academics and startups. Research of novel AI techniques requiring smaller data sets to train and that make more efficient use of compute could lead to important breakthroughs in the field. While increased investments in AI R&D are urgently necessary, this should not come at the expense of research in other disciplines. American competitiveness in the 21st century will depend on strong capabilities in a broad range of capabilities. Importantly, R&D investments in other sectors can enable better AI systems, creating a virtuous cycle of scientific advancement.

### 2NC --- Solves China

#### US AI RnD key to respond to Chinese AI challenges.

**Flournoy, Haines et al 2020 - former Under Secretary of Defense for Policy and Director of National Intelligence** [Michèle and Avril, Gabrielle Cheftiz Special Assistant to the Under Secretary of Defense for Policy October, “Building Trust through Testing Adapting DOD’s Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems” https://cset. georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf Acc 6/23/22 JZ]

Machine learning applications can increase the speed and quality of human decision-making on the battlefield, enable human-machine teaming to maximize performance and minimize the risk to soldiers, and greatly improve the accuracy and speed of analysis that relies on very large data sets. ML can also strengthen the United States’ ability to defend its networks against cyberattacks at machine speeds and has the power to automate critical components of labor-intensive enterprise functions, such as predictive maintenance and personnel management. Advances in AI and machine learning are not the sole province of the United States, however. Indeed, U.S. global leadership in AI remains in doubt in the face of an aggressive Chinese challenge in the field. Numerous DOD and academic reports reflect on the need to invest more in AI T 2 research and development, train and recruit a skilled workforce, and promote an international environment supportive of American AI innovation—all while promoting safety, security, privacy, and ethical development and use.

However, far too little attention is placed on the issue of trust, and especially testing, evaluation, verification, and validation (TEVV) of these systems. Building a robust testing and evaluation ecosystem is a critical component of harnessing this technology responsibly, reliably, and urgently. Failure to do so will mean falling behind.

### 2NC --- NATO fails

#### NATO slows down solvency due – only a unilateral plan avoids

Trabucco and Stanley-Lockman 21 [Lena -- L**ena** is a CSER Research Affiliate whose research examines the intersection of international security, international law, and emerging military technologies. and Zoe, ​**Zoe Stanley-Lockman** is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. Her research interests are in the areas of defence innovation, emerging technologies, defence industries, and military capability development. Previously she worked as a defence analyst at the European Union Institute for Security Studies in Paris and Brussels. She holds a Master's degree from Sciences Po Paris and a Bachelor's degree from Johns Hopkins University. Throughout her studies, her practical experience included working on dual-use export controls with the U.S. government and consulting for U.S. government systems integrators. Her participation in the *Warring with Machines*project will include framing machine learning in a socio-technical context that takes into account the unique aspects of defence economics, management, and operational environments, as well as applying lessons across alliances and like-minded countries. The Oxford Handbook of AI Governance, March, “NATO’s Role in Responsible AI Governance inMilitary Affairs”<https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb>-9780197579329-e-69] Blitz

Externally, as AI-enabled autonomous systems enter the arsenals of more technologically advanced countries, uncoordinated ethical frameworks between Allies could pose operational risks. Without wider alignment, AI systems will have “varying technical specifications based on the legal and policy decisions made by individual governments when answering the key questions.”[64](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-64) Further, although one motivation of autonomous systems is the increased safety of military personnel by removing them from dangerous situations, the lack of alignment could lead some Allies to perceive other capitals’ deployments of unmanned forces as a lack of commitment to put lives on the line, therein posing credibility risks for Allies to assure one another.[65](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-65) These credibility risks can be mitigated by accountability and verification standards and procedures that NATO can implement for multinational operations, and efforts to institutionalize these procedures for AI are underway.[66](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-66) While the NATO AI Strategy is expected to create a common foundation for the Alliance’s pursuit of AI, it is the implementation of principles for safe, ethical, legal, and interoperable AI that will reveal how coherent different national perspectives are. As of August 2021, only the United States and France have publicly issued their military AI strategies.[67](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-67) Other allies, including Canada and the United Kingdom, have emerging views on responsible military AI, but little official information about how they implement their ethical risk assessments is publicly available.[68](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-68)

### 2NC --- NIST

#### NIST is the best way to set standards – they are efficient and partner with academia

NIST 22 [NIST, National Institute for Science and Technology, "Plan for Federal AI Standards Engagement," NIST, https://www.nist.gov/artificial-intelligence/plan-federal-ai-standards-engagement] Blitz

NIST has released a [plan for prioritizing federal agency engagement in the development of standards for artificial intelligence (AI)](https://www.nist.gov/document/report-plan-federal-engagement-developing-technical-standards-and-related-tools) per the [February 2019 Executive Order on Maintaining American Leadership on Artificial Intelligence (EO 13859)](https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence). The plan recommends the federal government “commit to deeper, consistent, long-term engagement in AI standards development activities to help the United States to speed the pace of reliable, robust, and trustworthy AI technology development.”

It calls for federal agencies to bolster AI standards-related knowledge, leadership, and coordination among agencies that develop or use AI; promote focused research on the trustworthiness of AI systems; support and expand public-private partnerships; and engage with international parties.

NIST will participate in developing AI standards, along with the private sector and academia, that address societal and ethical issues, governance, and privacy policies and principles. These AI standards-related efforts include:

* Supporting and conducting AI research and development
* Actively engaging in AI standards development
* Procuring and deploying standards-based products and services, and
* Developing and implementing supportive policies, including regulatory policies where needed.

While the AI community has agreed that these issues must factor into AI standards, many decisions still need to be made about whether there is yet enough scientific and technical basis to develop those standards provisions.

## Norms

### 1NC --- UNESCO

#### UNESCO adopts cohesive AI policies

**Gaubert 21** [Julie Gaubert, Public Relations Author, 28/11/2021, UNESCO member countries adopt the first global agreement on the ethics of AI., EURONEWS,<https://www.euronews.com/next/2021/11/26/unesco-member-countries-adopt-first-global-agreement-on-the-ethics-of-artificial-intellige> MA]

Artificial intelligence (AI) is supporting the decision-making of governments, can help combat global issues such as climate change and give us personalised recommendations. But the UN agency **UNESCO also warns that the technology is bringing challenges, such as gender and ethnic bias, as well as threats to privacy.** It is because of this that **193 UNESCO member countries adopted the first global agreement on the ethics** **of artificial intelligence** on Thursday.**This is the "first global ethical framework for the use of artificial intelligence," said Audrey Azoulay, Director-General of UNESCO**. "AI technologies can be of great service to humanity" and "all countries can benefit from them", but "they also raise fundamental ethical concerns," the 28-page recommendation states. **There is a "need to ensure the transparency and intelligibility of the functioning of algorithms and the data from which they have been trained," because they can influence "human rights and fundamental freedoms,** gender equality and democracy," the Paris-based international organisation stated. Since the millennium**, AI has gradually made its way into our lives: it decides what news we read on our phones, which films are recommended to us on streaming services, or what routes GPS will take us on.** An expert group was set up in March 2020 to develop a draft recommendation on the ethics of AI. **The aim of the text is to "provide a responsible direction for AI technologies". "We see increased gender and ethnic bias, significant threats to privacy, dignity and agency, dangers of mass surveillance, and increased use of unreliable AI technologies** in law enforcement, to name a few. Until now, there were no universal standards to provide an answer to these issues," UNESCO said in a statement. In recent years, Meta (formally known as Facebook) has been at the centre of several scandals. The now shut-down British political consulting firm Cambridge Analytica was accused of misusing the US giant's data to politically influence the referendum in the United Kingdom and the election of Donald Trump in the US. **In light of this, the adopted text aims to guide the construction of the necessary legal infrastructure to ensure the ethical development of this technology. "The world needs rules for artificial intelligence to benefit humanity," Azoulay said. "The Recommendation on the ethics of AI is a major answer. It sets the first global normative framework while giving States the responsibility to apply it at their level. UNESCO will support its 193 Member States in its implementation and ask them to report regularly on their progress and practices".**

#### We solve modelling- UNESCO creates necessary incentives for Russia and China otherwise the aff gets circumvented

**Gaubert 21** [Julie Gaubert, Public Relations Author, 28/11/2021, UNESCO member countries adopt the first global agreement on the ethics of AI., EURONEWS,<https://www.euronews.com/next/2021/11/26/unesco-member-countries-adopt-first-global-agreement-on-the-ethics-of-artificial-intellige> MA]

**One pitfall of the agreement is that it does not impose anything on companies actively using artificial intelligence, particularly the US internet giants** Google, Amazon, Facebook, and Apple. David Leslie, a researcher at the Alan Turing Institute for Science and AI, nevertheless saw it as "a step in the right direction". H**e believes believed other international institutions, such as the Council of Europe and the European Union, will soon follow UNESCO's model.** "Texts like this one put a lot of pressure on the Facebooks of this world, whose "predatory behaviour is increasingly exposed," Leslie said. "Acting with as much impunity as Facebook has done is no longer possible". **However, UNESCO does not directly address the subject of facial recognition. This is a central theme that the European Union has taken up.** The European Commission is proposing [**a strictly regulated use**](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206) of remote biometric identification systems in public places. Meanwhile, **Russia, China, and Iran - states regularly accused of obstructing human rights - are signatories to the text, which UNESCO acknowledges is an "incentive mechani**sm" without the possibility of sanctions. "If this text had no power, these countries would not even have come to discuss it," Alessandra Sala, director of the artificial intelligence service of content provider Shutterstock, said. **These three countries ratified the recommendation "because they realise that we are at a pivotal moment in AI and they don't want to be seen as the countries going in the wrong direction," she added.** The United States and Israel, which are very active in new technologies, are not UNESCO member states. **But the US is working on AI legislation and is "ahead of Europe," said Sala.**

### 2NC --- Solvency

#### UNESCO has already taken the lead on AI, the counter plan furthers these efforts which solves the aff

**Abhishree Choudhary 12 – 21** - Connor McPartland is an assistant director with the Atlantic Council’s Transatlantic Security Initiative, part of the Scowcroft Center for Strategy and Security.

[“Ethics Of AI: 193 Members Of UNESCO Adopt Recommendations” https://analyticsindiamag.com/ethics-of-ai-193-members-of-unesco-adopt-recommendations/ - Acc 6-19-22 JZ]

In a historic global agreement, all 193 members of UNESCO adopt the recommendations on the ethics of AI document

In a historic global agreement on 25 November 2021, all 193 members of the United Nations Educational, Science and Cultural Organisation adopted the “Recommendation on the ethics of artificial intelligence”. However, the recommendations are not a binding agreement, rather guidelines that nations can follow voluntarily.

The document acknowledges the “profound and dynamic” impact of AI on human lives and contemporary societies and how it affects education, social and natural sciences, culture, etc.

Moreover, UNESCO recognises the potential that AI possesses in terms of benefitting ecosystems and the environment.

On the other hand, UNESCO, in its document, highlights the dangers of AI. It raises ethical concerns surrounding the gender and ethnic biases that are “embedded” in algorithms which may “exacerbate” inequality, exclusion and threats to cultural, social and ecological diversity. The document further raises AI red flags by stating that AI technology may deepen a divide between countries.

In this regard, UNESCO Chief Audrey Azoulay says, “The world needs rules for artificial intelligence to benefit humanity. The Recommendation on the ethics of AI is a major answer. It sets the first global normative framework while giving States the responsibility to apply it at their level.”

### 2NC --- Modelling

#### CP solves modelling, coordinating through UNESCO provides a specific universal framework for AI usage

Ethics of AI: Values and Principles

The document defines the scope and provides a universal framework of values and principles of the ethics of AI within its scope. The definition of AI within the document includes and is not limited to machine learning, machine reasoning, cyber-physical systems, IoT, and all stages of AI systems life cycle (process, person, enterprise).

The objective of the document is to guide the actions of the stakeholders in embedding the ethics of the AI, promote human rights and fundamental freedom in all stages of the AI life cycle, and promote equitable access to development and knowledge in the field of AI between the global north and south nations. The recommendations explicitly ban the use of AI social scoring and mass surveillance and advocate stronger data protection.

The text principally calls for:

Fairness and Non-Discrimination- Fairness implies sharing the benefits of AI technologies at local, national and international levels while considering the specific needs of different marginalised and vulnerable populations.

Sustainability- AI technologies must be continually assessed for their social, cultural, economic and environmental impact.

Privacy– Human autonomy and agency must be respected, and data must be collected, shared, archived and deleted ethically. The document also calls for data protection through frameworks and government mechanisms set up by regulatory bodies. In addition, algorithmic systems must undergo privacy impact assessment, which includes societal and ethical considerations.

Safety and Security– Unwanted harm and vulnerability to attack should be avoided by developing privacy-protective data access frameworks that foster better training AI models.

Transparency and Explainability- Transparency ensures respect for human rights principles. Explainability refers to making intelligible and insightful outcomes to the AI system.

Responsibility and Accountability- Similar to transparency and explainability, the principle ensures human rights and freedom.

Awareness and Literacy- Public awareness and understanding of AI technologies and the value of data must be promoted through open and accessible education to all.

Political Scenario

Interestingly, nations like China and Russia who have a comprehensive mass surveillance system, have voted to adopt AI Ethics Recommendations. The USA, a country that houses the most number of AI companies, is not a part of UNESCO, thus, not a signatory to the document. However, in an interview with Politico, UNESCO’s Assistant Director-General for Social and Human Sciences, Gabriela Ramos, argues that the nation’s policies can be pressured by global unity on the subject.

### 2NC --- NATO follow on

#### AND the US is a global AI leader – it establishes norms and countries follow on consistent with NATO

Parker 20 [Lynne Parker, Dr. Lynne Parker is Director of the National Artificial Intelligence Initiative Office, Deputy United States Chief Technology Officer, and Assistant Director of Artificial Intelligence at the White House Office of Science and Technology Policy (OSTP). She is detailing to OSTP from her position as Professor in the Department of Electrical Engineering and Computer Science at the University of Tennessee, Knoxville (UTK). She previously served as Interim Dean of the Tickle College of Engineering (TCE) at UTK, and before that was the Associate Dean for Faculty Affairs and Engagement in TCE. She also previously served at NSF as Division Director of Information and Intelligent Systems. She spent several years at Oak Ridge National Laboratory as a Distinguished Research and Development Staff Member. She received her PhD in Computer Science from the Massachusetts Institute of Technology. "The American AI Initiative: The U.S. strategy for leadership in artificial intelligence," No Publication, https://oecd.ai/en/wonk/the-american-ai-initiative-the-u-s-strategy-for-leadership-in-rtificial-intelligence] Blitz

On February 11, 2019, President Donald J. Trump launched the [American Artificial Intelligence Initiative,](https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/)the United States’ national strategy for maintaining American leadership in AI, by signing [Executive Order 13859.](https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence)This blog post details how that initiative recognizes the importance of American leadership in AI to maintain the economic and national security of the United States and to shape the global evolution of AI in a manner consistent with our Nation’s values, policies, and priorities. **United States policies and practices to promote trustworthy AI innovation** The American AI Initiative focuses the resources of the Federal Government in support of AI innovation that will increase prosperity, enhance national security, and improve quality of life. In the past year since the signing of the Executive Order, the United States has made significant progress on achieving the national strategy‘s objectives. This national strategy is well-aligned with the OECD AI Principles and takes important action to support the development of trustworthy AI. The Initiative emphasizes the following key policies and practices: ***Invest in AI research and development:*** The United States must promote Federal investment inAI R&D in collaboration with industry, academia, international partners and allies, and other non-Federal entities to generate technological breakthroughs in AI. President Trump called for a two-year [doubling of non-defense AI R&D in his fiscal year 2021 budget proposal,](https://www.whitehouse.gov/briefings-statements/president-trumps-fy-2021-budget-commits-double-investments-key-industries-future/) and in 2019 the Administration [updated its AI R&D strategic plan,](https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf) developed the first [progress report](https://www.whitehouse.gov/wp-content/uploads/2019/11/AI-Research-and-Development-Progress-Report-2016-2019.pdf) [describing the impact of Federal R&D investments,](https://www.whitehouse.gov/wp-content/uploads/2019/11/AI-Research-and-Development-Progress-Report-2016-2019.pdf) and published the first-ever reporting of government-wide non-defense AI R&D spending. ***Unleash AI resources****:*The United States must enhance access to high-quality Federal data,models, and computing resources to increase their value for AI R&D, while maintaining and extending safety, security, privacy, and confidentiality protections. The American AI Initiative directs Federal agencies to [identify new opportunities](https://www.federalregister.gov/documents/2019/07/10/2019-14618/identifying-priority-access-or-quality-improvements-for-federal-data-and-models-for-artificial) to increase access to and use of Federal data and models. In 2019, the White House Office of Management and Budget established the [Federal Data Strategy](https://strategy.data.gov/)as a framework for operational principles and best practices for Federal agencies and how they use and manage data. ***Remove barriers to AI innovation****:*The United States reduces barriers to the safedevelopment, testing, deployment, and adoption of AI technologies by providing guidance for the governance of AI consistent with our Nation’s values and by driving the development of appropriate AI technical standards. As part of the American AI Initiative, The White House proposed the [United States AI Regulatory Principles,](https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf) a first-of-its-kind national AI regulatory policy that advances innovation underpinned by American values. In addition, the National Institute of Standards and Technology (NIST) issued the first-ever [strategy for Federal engagement in the development](https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf) [of AI technical standards.](https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf) ***Promote an international environment supportive of American AI innovation****:* The United States engages internationally to promote a global environment that supports American AI research and innovation and opens markets for American AI industries while ensuring that AI is developed in a matter consistent with our Nation’s values, including protecting privacy, civil rights, and civil liberties. Last year, the United States joined with allies in historic efforts at the Organisation for Economic Cooperation and Development (OECD) to develop the first [intergovernmental](http://www.oecd.org/going-digital/ai/principles/) [consensus agreement on fundamental principles for the stewardship of trustworthy AI.](http://www.oecd.org/going-digital/ai/principles/) The United States supports OECD’s ongoing work to implement these principles through the AI Policy Observatory and related activities. ***Embrace trustworthy AI for government services and missions****:* The United States embraces technology such as artificial intelligence to improve the provision and efficiency of government services to the American people and ensure its application upholds our Nation’s values, including protecting privacy, civil rights, and civil liberties. The General Services Administration established an [AI Center of Excellence](https://coe.gsa.gov/coe/artificial-intelligence.html) to enable Federal agencies to determine best practices for incorporating AI into their organizations. ***Train an AI-ready workforce****:*The United States empowers current and future generationsof American workers through apprenticeships; skills programs; and education in science, technology, engineering, and mathematics (STEM), with an emphasis on computer science, to ensure that American workers are capable of taking full advantage of the opportunities of AI. President Trump directed all Federal agencies to prioritize AI-related apprenticeship and job training programs and opportunities. In addition to its R&D focus, the National Science Foundation’s new [National AI Research Institutes](https://www.nsf.gov/news/news_summ.jsp?cntn_id=299329&org=NSF&from=news) program will also contribute to workforce development, particularly of AI researchers. America’s strong innovation ecosystem, fuelled by strategic Federal investments, visionary scientists and entrepreneurs, and renowned research institutions, has propelled the United States to global leadership in AI. However, continued leadership is not predetermined. Maintaining America’s preeminent role in AI can only be realized by continually building upon our progress and pursuing a strategic, forward-looking approach in partnership with industry, academia, non-profit organizations, other non-Federal entities, and like-minded international allies. Together, we will shape the trajectory of AI development for good — enriching our lives, promoting innovation, fostering trust and understanding, and ensuring our national defense and security. NATO slows down solvency and causes cohesion – only a unilateral plan avoids Trabucco and Stanley-Lockman 21 [Lena -- L**ena** is a CSER Research Affiliate whose research examines the intersection of international security, international law, and emerging military technologies. and Zoe, ​**Zoe Stanley-Lockman** is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. Her research interests are in the areas of defence innovation, emerging technologies, defence industries, and military capability development. Previously she worked as a defence analyst at the European Union Institute for Security Studies in Paris and Brussels. She holds a Master's degree from Sciences Po Paris and a Bachelor's degree from Johns Hopkins University. Throughout her studies, her practical experience included working on dual-use export controls with the U.S. government and consulting for U.S. government systems integrators. Her participation in the *Warring with Machines* project will include framing machine learning in a socio-technical context that takes into account the unique aspects of defence economics, management, and operational environments, as well as applying lessons across alliances and like-minded countries. The Oxford Handbook of AI Governance, March, “NATO’s Role in Responsible AI Governance inMilitary Affairs”<https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb>-9780197579329-e-69] Blitz Externally, as AI-enabled autonomous systems enter the arsenals of more technologically advanced countries, uncoordinated ethical frameworks between Allies could pose operational risks. Without wider alignment, AI systems will have “varying technical specifications based on the legal and policy decisions made by individual governments when answering the key questions.”[64](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-64) Further, although one motivation of autonomous systems is the increased safety of military personnel by removing them from dangerous situations, the lack of alignment could lead some Allies to perceive other capitals’ deployments of unmanned forces as a lack of commitment to put lives on the line, therein posing credibility risks for Allies to assure one another.[65](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-65) These credibility risks can be mitigated by accountability and verification standards and procedures that NATO can implement for multinational operations, and efforts to institutionalize these procedures for AI are underway.[66](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-66) While the NATO AI Strategy is expected to create a common foundation for the Alliance’s pursuit of AI, it is the implementation of principles for safe, ethical, legal, and interoperable AI that will reveal how coherent different national perspectives are. As of August 2021, only the United States and France have publicly issued their military AI strategies.[67](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-67) Other allies, including Canada and the United Kingdom, have emerging views on responsible military AI, but little official information about how they implement their ethical risk assessments is publicly available.[68](https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780197579329.001.0001/oxfordhb-9780197579329-e-69#oxfordhb-9780197579329-e-69-note-68)

## EU

### AI Act

#### Following onto the EU AI Act

**Townsend 21** [Bev Townsend, Postdoctoral Researcher at University of York, “Decoding the Proposed European Union Artificial Intelligence Act”, Insights, <https://eprints.whiterose.ac.uk/178738/1/Townsend_Decoding_the_Proposed_EU_AI_Act_ASIL_Insights.pdf>, JMH]

The Proposed Regulation Laying Down Harmonised Rules on Artificial Intelligence On April 21, 2021, the European Commission published the highly anticipated proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act or the Act).11 This followed the Commission’s ongoing commitment to establish “legislation for a coordinated European approach on the human and ethical implications of AI.”12 At the outset it is worth noting that, rather than focusing on the properties or outcomes of AI, the Act defines an “AI system” as software that is developed using certain techniques and approaches (detailed in an annex) that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.13 Any AI system developed not using one of the enumerated techniques or approaches falls outside of the definition—a definition that, because of its imprecision, creates the opportunity to skilfully circumvent the Act. The intention is for the new legal framework to provide a set of harmonised rules that align (and are consistent with) existing EU human rights instruments and EU law regulating data protection, data governance, consumer protection, non-discrimination, and gender equality. Accordingly, a cautious yet balanced and proportionate regulatory approach is proposed, one that is primarily risk-based. It sets out the minimum necessary requirements to address risks to values, fundamental rights, and principles associated with AI development and deployment without unnecessarily constraining technological development or trade.14 What the Act does—and does well—is to differentiate requirements by risk level and to prohibit more objectionable AI systems that carry what is considered “undesirable risk” of fundamental rights infringement. The Act also introduces new legal obligations (such as monitoring, reporting, and transparency obligations) to manage those systems that, although not prohibited, are considered high risk. Amongst others, the Act establishes a robust governance, monitoring, and enforcement regime, sets up a European Artificial Intelligence Board, and seeks to impose sanctions and penalties for non-compliance. Adopting a Risk-Based Approach: The Level of Risk Determines the Applicable Rules. The central tenet of the AI Act is to introduce a set of binding rules based upon the intensity and scope of the risk generated by the AI system. The impetus for such a riskdriven approach is that persons at risk and vulnerable to health, safety, and rights infringement by new AI technologies require a higher level of protection. This is premised on the understanding that AI systems have certain characteristics (inter alia, an opacity, complexity, dependency on data, and capacity for autonomous behaviour) that can adversely and significantly affect fundamental human rights—rights to data privacy, transparency, autonomy, and the like.15 The Act addresses three categories of risk: 1. Prohibited Systems. Prohibited systems include AI systems that manipulate human behavior and/or exploit persons’ vulnerabilities; social scoring systems; and, save for certain exceptions, “real-time” and “remote” biometric identification (or facial recognition) systems. 2. High-Risk Systems. While not clearly defined, a “high-risk” system is understood to be one that poses significant risk to health, safety, and fundamental rights. Although the AI Act applies generally to all AI systems, certain provisions contained within the Act (and provided for in Title III) apply specifically to those considered high-risk. High-risk systems are either those products (or safety components of products) already covered by EU health and safety harmonisation legislation (such as medical devices, toys, and machinery, for instance) or those AI systems used in specified areas and contained in an annex to the Act (such as educational training, employment, and law enforcement).16 Rather than relying on certain criteria to position a system as high-risk, the Act designates as high-risk all AI systems used within a specified enlisted and pre-determined domain. There are also no gradations of high-risk systems—either a system is high-risk, in which case compliance with a comprehensive list of requirements and obligations is prescribed, or it is not. Once it has been established that an AI system is high-risk, it is mandated that the system’s provider (the person, agency, or body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark17) must fulfill certain requirements and obligations. These requirements include that quality and risk management systems be implemented; that training, validation, and testing datasets be subject to appropriate data governance and management practices and meet data quality criteria; that technical documentation be drawn up and proper records be kept; and that transparency obligations be fulfilled.18 These obligations are set out in detail within the Act. An important further requirement is that high-risk AI systems be designed and developed to allow for human oversight so that natural persons can oversee their functioning. Providers are required to introduce “human-machine interface tools” and measures to guarantee that a system is subject to built-in operational constraints that cannot be overridden by the system itself and is responsive only to a human operator. 3. Low- or Minimal-Risk Systems. All other AI systems that are without risk, or are of low or minimal risk, can be developed, sold, and deployed without additional legal obligations subject, of course, to compliance with any existing relevant legislation (including data protection legislation, such as the GDPR). Moreover, those that design and deploy low- or minimal-risk systems are encouraged to adhere to voluntary codes of conduct. Disclosing Bots, Detecting Emotions, and Deep Fakes Although there are no special requirements for low-risk systems, transparency obligations apply to all risk-levels, and three categories of disclosable activities are distinguished. First, providers of AI systems must design systems so that natural persons are informed that they are interacting with an AI system (so-called robot or “bot” disclosures). This disclosure is to avoid any potential confusion by a natural person when interacting with an AI system. It is not necessary to make such a disclosure in instances where it is contextually obvious that persons are interacting with an AI system. Second, users of systems that detect emotions or determine association with (social) categories based on biometric data must be informed of the operation of the system except in instances permitted by law or in crime prevention. And lastly, although certain exemptions apply, it is required that creators of artificial images, video, or audio content disclose that they have been generated synthetically or manipulated, such as in the case of “deep fakes.”19 Extraterritorial Reach Crucially, if adopted in its proposed form, the AI Act, much like the GDPR, will be farreaching and have significant consequences beyond the EU. The Act has extraterritorial effect and, subject to certain specific exceptions, applies to: (i) providers that place on the market or deploy AI systems in the EU, regardless of where such providers are located; (ii) users of AI systems located within the EU; and (iii) providers and users of AI systems that are located outside the EU to the extent that the output produced by the system is used within the EU. Conclusion: A Step in the Right Direction If the AI Act is strikingly similar to the GDPR, it is perhaps no coincidence. Is the AI Act likely to become the new global “gold standard” for the adoption of AI regulation? Will the EU be the sole and dominant crafters of the laws governing technology? Certainly, many low- and medium-resource countries look to regulations such as those promulgated by the EU to guide and inform their new regulatory policy development. To this end, and despite various shortcomings, the Act is a valuable start in helping to shape global norms and standards and promote trustworthy AI—AI systems that are, at least to some degree, more consistent with human values and interests. The Act also promotes innovation, including regulatory sandboxes and specific measures to support small-scale users and providers. Some may say that in preserving rights it does not go far enough, while innovators and developers may argue that it goes too far. But promoting ethical innovation and fair competition while balancing rights is not easily done— compromise is often needed—and the right regulatory framework should (prudently) do both. But by covering too much ground—fundamental rights, health and safety, data protection, and consumer law—there is a risk that the practical operationalisation and implementation of the law may be untenable. Further, a plausible framework should also be nuanced and flexible enough to adapt to, and keep abreast of, the rapidly evolving landscape that is AI development and deployment. Whether the AI Act does this sufficiently in its present form remains to be seen.

### OECD Cards (NATO SAYS NO)

#### NATO SAYS NO- US Government working towards better security co-op w/ OECD

**Carayannis & Draper 22** [E.G. Carayannis & J. Draper, American Scientist & Austhor, 11 January 2022, Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence, AI & Soc,<https://doi-org.proxy.lib.umich.edu/10.1007/s00146-021-01382-y>, 6/19/2022 MA]

**Canada and the United States joined forty other countries in adopting the first ever set of intergovernmental rules on the use of artificial intelligence (**AI) at a conference in Paris on Wednesday, as the technology promises potential benefit and fuels ethical and other concerns. The [four-page document](https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449) **the nations' representatives put their signatures to stresses AI should be developed and implemented fairly and safely, urging governments to create policies for “responsible stewardship of trustworthy AI.”** The guidelines were **drafted through an initiative led by the Organization for** **Economic Cooperation and Development (OECD**), which brought together more than 50 experts from industry, 20 governments, civil society and tech companies. They aim to provide a stable environment for the development and implementation of AI through shared fundamental values. “AI technology is still in its infancy and its potential remains to be realized," OECD Secretary-General Angel Gurría said at the official adoption of the principles on 22 May. "And while AI is driving optimism, it is also fueling anxiety and ethical concerns,” he added. **The principles include five value**-**based principles for the development of AI** and five recommendations for public policy**. The document states that AI should benefit people and planet** **and be designed in a way that respects the rule of** **law, human rights, democratic values and diversity**. AI systems should be transparent and safe. Their risks should continually be assessed and managed. And those developing, deploying or operating AI systems should be held accountable for their use of the technology,it reads. **The OECD experts also recommend that governments facilitate investment in research and development, foster accessibility to AI systems by sharing data and knowledge, create policy to ensure citizens trust in AI systems, train displaced people** **with skills to help with smoother economic transition, cooperate** **with other governments to share best practices**. Artificial intelligence is already displacing some human employment, and unease about how far that trend will go will need to be dealt with as its application to more problems grows. As a general purpose technology it will affect all fields, and so the principles deal with all the potential consequences and benefits of AI from the economic impact for workers to how data gathered will be used for healthcare, traffic management, advertising or any other purposes. **The principles are not legally binding** but **it will allow the OECD to monitor** and compare **the progress of the 42 signatories in their development and use of AI**. The OECD also has a history of producing policy documents that contribute to later national and international legislation. Their [1980 privacy guidelines](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf), which highlighted the need to set limits on **the collection and use of personal data, was the groundwork policy which the European Union considered for its General Data Protection Regulation law. The OECD is a 36-member club of developed countries that describe themselves as committed to democracy** **and the market economy.** All members signed the AI document, as did Argentina, Brazil, Colombia, Costa Rica, Peru and Romania. OECD officials in charge of the initiative said they were satisfied that many countries worked together to develop and agree to the principles and they hoped more countries will adopt them. “Our ambition goes far beyond our membership,” said Andrew Wyckoff, director for science, technology and innovation at the OECD.

#### Even without NATO OECD can fill in on AI.

**Carayannis & Draper 22** [E.G. Carayannis & J. Draper, American Scientist & Austhor, 11 January 2022, Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence, AI & Soc,<https://doi-org.proxy.lib.umich.edu/10.1007/s00146-021-01382-y>, 6/19/2022 MA]

While **the United States under President Donald Trump has been pulling away from international agreements and institutions such as the Paris climate accord, NATO, and the UN, U.S. government officials participated in the drafting of the principles which the country later agreed to adopt**. U.S. President Donald Trump himself had called for [regulating AI in an executive order](https://www.nytimes.com/2019/02/11/business/ai-artificial-intelligence-trump.html) in February. The executive order also aimed to promote cooperation with foreign powers. **An official at the OECD also said the United States adopted the principles because they wanted to keep some control over international agreements on technology and were worried that Europeans were becoming the global rule-setters since the General Data Protection Regulation.** “During the whole process of negotiation, the US have been making compromises with the other countries and stakeholders,” said Anne Carblanc, head of the OECD's digital economic policy division. The United States is home to some of the world’s biggest technology companies such as Google, Amazon, Facebook and Apple. China is its main competition with the [second most investment in AI startups](https://www.nytimes.com/2019/02/11/business/ai-artificial-intelligence-trump.html). The country, which is not a member of the OECD, sees AI through different eyes. The country has used [the technology to increase surveillance on its population](https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html), among other uses. **Gurría, the OECD's secretary-general, confirmed** **more general fears around the development of AI.** "There are questions around the trustworthiness, the robustness of AI systems including the dangers of codifying or reinforcing existing biases related to gender, race, or infringing on human rights of important values like privacy," he said during his opening address. The United States was among signatories keen for the document to reinforce democratic values centred on human rights, officials said. “With [their participation], **the US was keen on establishing a certain path that was more in line with the OECD and our values,” said Wyckoff.**

#### CP solves- it models off existing EU negotiations that are necessary for further cooperation with NATO

**Carayannis & Draper 22** [E.G. Carayannis & J. Draper, American Scientist & Austhor, 11 January 2022, Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence, AI & Soc,<https://doi-org.proxy.lib.umich.edu/10.1007/s00146-021-01382-y>, 6/19/2022 MA]

Artificial intelligence has been a focus of international discussions this year, and the OECD AI principles will be discussed at a G20 summit in Japan on June 28 and 29. **OECD officials and experts are developing a more practical document for the implementation of the principles. Artificial intelligence has also been the focus of the G7 hosted by France. The country’s president Emmanuel Macron has partnered with Prime Minister Justin Trudeau’s government to push for strong cooperation.** In late 2018, both countries announced the creation of a group of international experts on AI, which would be modeled after the International Panel on Climate Change. During a G7 meeting of ministers of digital affairs **in May, Canada and France unveiled** [**more details**](https://www.canada.ca/en/innovation-science-economic-development/news/2019/05/canada-and-france-work-with-international-community-to-support-responsible-use-of-artificial-intelligence.html) **about future international group IPAI (International Panel on Artificial Intelligence). The European Union unveiled its** [**Ethics Guidelines for Trustworthy AI**](https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai) **in April.** The document, **which establishes consensus among EU members, mentions the importance of human agency and oversight of AI systems and the need to ensure respect for privacy and data protection. The document ​​​​represents a first step toward practical guidelines and potential regulation in the future.**

#### More follow through – successful security cooperation & AI agreement among US and EU

**Carayannis & Draper 22** [E.G. Carayannis & J. Draper, American Scientist & Austhor, 11 January 2022, Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence, AI & Soc,<https://doi-org.proxy.lib.umich.edu/10.1007/s00146-021-01382-y>, 6/19/2022 MA]

While **the United States under President Donald Trump has been pulling away from international agreements and institutions such as the Paris climate accord, NATO, and the UN, U.S. government officials participated in the drafting of the principles which the country later agreed to adopt**. U.S. President Donald Trump himself had called for [regulating AI in an executive order](https://www.nytimes.com/2019/02/11/business/ai-artificial-intelligence-trump.html) in February. The executive order also aimed to promote cooperation with foreign powers. **An official at the OECD also said the United States adopted the principles because they wanted to keep some control over international agreements on technology and were worried that Europeans were becoming the global rule-setters since the General Data Protection Regulation.** “During the whole process of negotiation, the US have been making compromises with the other countries and stakeholders,” said Anne Carblanc, head of the OECD's digital economic policy division. The United States is home to some of the world’s biggest technology companies such as Google, Amazon, Facebook and Apple. China is its main competition with the [second most investment in AI startups](https://www.nytimes.com/2019/02/11/business/ai-artificial-intelligence-trump.html). The country, which is not a member of the OECD, sees AI through different eyes. The country has used [the technology to increase surveillance on its population](https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html), among other uses. **Gurría, the OECD's secretary-general, confirmed** **more general fears around the development of AI.** "There are questions around the trustworthiness, the robustness of AI systems including the dangers of codifying or reinforcing existing biases related to gender, race, or infringing on human rights of important values like privacy," he said during his opening address. The United States was among signatories keen for the document to reinforce democratic values centred on human rights, officials said. “With [their participation], **the US was keen on establishing a certain path that was more in line with the OECD and our values,” said Wyckoff.** Artificial intelligence has been a focus of international discussions this year, and the OECD AI principles will be discussed at a G20 summit in Japan on June 28 and 29. **OECD officials and experts are developing a more practical document for the implementation of the principles. Artificial intelligence has also been the focus of the G7 hosted by France. The country’s president Emmanuel Macron has partnered with Prime Minister Justin Trudeau’s government to push for strong cooperation.** In late 2018, both countries announced the creation of a group of international experts on AI, which would be modeled after the International Panel on Climate Change. During a G7 meeting of ministers of digital affairs **in May, Canada and France unveiled** [**more details**](https://www.canada.ca/en/innovation-science-economic-development/news/2019/05/canada-and-france-work-with-international-community-to-support-responsible-use-of-artificial-intelligence.html) **about future international group IPAI (International Panel on Artificial Intelligence). The European Union unveiled its** [**Ethics Guidelines for Trustworthy AI**](https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai) **in April.** The document, **which establishes consensus among EU members, mentions the importance of human agency and oversight of AI systems and the need to ensure respect for privacy and data protection. The document ​​​​represents a first step toward practical guidelines and potential regulation in the future.**

### BIPARTISAN AI POLICY

#### Adoption of Bipartisan Policies = more coherent AI strategies

**Rao &**<https://www.pwc.com/us/en/contacts/b/bret-greenstein.html> **Greenstein 22** [Ananad Rao & Brey [Greenstein](https://www.pwc.com/us/en/contacts/b/bret-greenstein.html), Global AI Lead; US & Data and Analytics Partner, 2022, PwC 2022 AI Business Survey, PWC,<https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-business-survey.html?WT.mc_id=CT3-PL300-DM1-TR1-LS4-ND30-PRG7-CN_DataAndAnalyticsBuilds-AISurveyGoogle&gclsrc=aw.ds&gclid=Cj0KCQjwkruVBhCHARIsACVIiOzHzJE67Rf53JLr1GSKxGKh89BRHWtLVNxoQh7RJoPTtlKmzjb7ZgAaAgxFEALw_wcB>, 6/24/2022, MA]

**Companies that take a more holistic approach to AI, focusing on achieving three business goals, see greater success than those that take a singular approach.** Bar chart titled Compared to companies that approach AI in a piecemeal manner, these leaders (just over a third in our survey) are far more likely (36% versus 20%) to report widespread AI adoption. **They’re roughly twice as likely to rep9ort substantial value from AI initiatives to improve productivity, decision-making, customer experience, product and service innovation, employee experience and more. By bringing so many leaders together from across the organization,** a holistic approach facilitates scale and data sharing. It brings together AI specialists with analytics teams, software engineers and data scientists. By including business experience, it helps align outcomes with business priorities, leading to organizational buy-in and to projects that deliver a real impact at a reasonable cost. This holistic approach supports a critical ingredient **of AI success: investing in and managing data, AI and cloud as a unified whole. AI can deliver more value at scale when it’s embedded in application systems that work nonstop, analyzing and acting on data from inside and outside the organization.** These systems, in turn, need cloud-based computing power that can scale up and down to help meet demands. An approach to AI initiatives that encompasses business, technology and decision-making priorities helps data, AI and cloud work together smoothly, end-to-end. This unified approach to **AI aligns well with a unified approach to data: making a person (such as a chief data officer) or a centralized team responsible for data sharing and data governance. That can help connect data to AI in ways that benefit as many lines of business as possible. Thirty-six percent of companies with a holistic approach to AI are planning to use AI this year to help create a data fabric: an action-ready, 360-degree view of all data that touches their organizations.** Within this framework, many AI leaders plan to focus on five key priorities, all related to one theme: delivering valuable, real-world business outcomes. AI-supported decision-making is so powerful for a simple reason: it can enable you to incorporate and analyze far more information than you (or any human being) could do on their own. To help optimize pricing, for example, AI can input reams of historical data on product sales, margins, supplier costs and customer satisfaction, then produce rigorous estimates of possible future scenarios. It can project how competitors and suppliers might change their prices in response to your decisions. AI combined with Internet of Things (IoT) sensors can forecast machines’ performance and maintenance needs, enabling better operational decisions. With the rise in “AI at the edge” — **AI combined with edge computing, so AI algorithms are executed at or near the device level — these decisions can be lightning fast, too. Start with outcomes.** As you consider new AI models in decision-making, don’t start with the data you have. Instead, start with the business outcome you seek, then look for the data and analytics to back it up. **Consider which decision-makers will use the model to achieve this outcome, where the model will fit within the decision-making process, how it will integrate with the cloud, and how you will monitor, scale, improve and eventually retire it. Let AI make your data actionable.** Once you’ve identified the data you need, let AI help you find and use it. Many companies are drowning in unstructured, “messy” data. Whether with [**documents**](https://www.youtube.com/watch?v=o5_iO4gHoUo), images or video, AI can wade through this ocean of data, extract exactly what decision-makers need and put this data — and only this data — in front of the right people at the right time. **Focus, then scale. A holistic approach doesn’t mean “everything at the same time.” An effective way to use AI in highly complex decisions, such as ESG, is to start with a specific element, such as a single facility’s carbon footprint. You can then scale up to other facilities and ESG factors**.What companies can do **Create synthetic data.** Machine learning models require huge amounts of data — which simulation models can create. For facial recognition, for example, instead of acquiring images of faces from multiple angles, contrast levels and brightness, simulations can generate them to train machine learning models. **Synthetic data, which AI simulations can provide, can turbocharge other AI and analytics initiatives. Make digital twins a platform too.** To effectively use AI’s power to create business-relevant simulations, consider (as part of AI’s integration with [**data platforms**](https://www.pwc.com/us/en/products/insights-platform.html) and [**cloud**](https://www.pwc.com/us/en/tech-effect/cloud/cloud-business-survey.html)) making digital twins a platform capability — to help make sense of your various data sets in the context of your business, your customers and your products**. Align your specialists. Your simulation specialists very likely have an engineering background, while your data scientists will typically be more experimental scientists. Bringing these specialists together with each other and with business leaders is key to solving simulation problems.**  Companies are now increasingly able to answer these and other questions, thanks to new assessment methods. These can capture not just “hard” returns, such as increased productivity, and “hard” costs, such as new hardware spending. They can also capture “soft” returns, such as an improved employee experience, and “soft” costs, such as increased demands on subject matter specialists’ time. The holistic approach to AI, by fostering scale, shared insights and shared leading practices, also makes it easier to predict the ROI of new initiatives. As you work to measure and increase AI’s ROI, you may also be able to take advantage of AI itself: its simulations can model the uncertainties that surround other AI initiatives, helping to better allocate resources. What companies can do **Be complete.** As you use the [**new methods**](https://www.pwc.com/us/en/tech-effect/ai-analytics/artificial-intelligence-roi.html) to assess and predict AI’s ROI, be sure to factor in uncertainties (such as AI models’ exact error rate), changes in model performance and maintenance needs over time, and how different AI initiatives could impact each other’s results. **Build a portfolio.** To help avoid ROI surprises, consider a [**portfolio approach**](https://www.pwc.com/us/en/tech-effect/ai-analytics/how-ai-portfolio-helps-roi.html): as you might do with financial investments or product innovation, create and assess a mix of initiatives that will raise the likelihood of delivering the overall results you need. **Manage the life cycle.** **To further predict and boost AI’s ROI, aim to manage not individual AI projects, but an integrated data-AI-cloud (DAC) life cycle. That can help you continually evolve strategy, fine-tune execution and find new use cases for data — both avoiding downside surprises and identifying new value. Given the widespread understanding of** [**responsible AI’s urgency**](https://www.pwc.com/gx/en/issues/data-and-analytics/artificial-intelligence/what-is-responsible-ai.html), the lack of action likely reflects the challenges. Responsible AI requires both technology and business experience. AI professionals may, for example, miss the impact on compliance or the brand when AI makes decisions based on historical data sets, which may be rife with historically common biases. Business and risk experts may lack the technical skills to forecast how highly complex algorithms may perform as circumstances change. **And since AI continuously evolves its own decision-making based on new data, it requires governance and protection that evolve too. What companies can do Govern the life cycle.** To keep up with fast-changing AI models, deploy [**end-to-end governance**](https://towardsdatascience.com/top-down-and-end-to-end-governance-for-the-responsible-use-of-ai-c67f360c64ba) of the DAC life cycle.. This governance should integrate risk, AI and business leaders, with new procedures, roles and responsibilities for each of your three lines of defense. **You often can employ and enhance much of existing IT governance and controls, but many business and risk leaders may need to learn some AI and data science basics. Assess the impact.** To facilitate the work of integrated teams and life-cycle governance, consider [**algorithmic impact assessments**](https://www.pwc.com/us/en/tech-effect/ai-analytics/algorithmic-impact-assessments.html)**. By evaluating the end-to-end AI life cycle, they can capture risk, identify governance needs, increase accountability and facilitate go/no-go decisions. Minimize bias. Many companies today are understandably focusing on responsible AI basics: making sure that AI is safe and does what it’s supposed to. But as AI supports ever more business-critical decision making, it will likely become increasingly important to** [**decrease AI bias**](https://www.pwc.com/us/en/tech-effect/ai-analytics/algorithmic-bias-and-trust-in-ai.html)**, so that your AI models treat all of your stakeholders fairly approach to be continuing full speed ahead with AI initiatives despite the AI talent shortage (23% versus 14%). That may be because they’re far more likely to be pursuing leading practices such as retraining in-house** **talent to work with AI** (43% versus 33%), and reorganizing teams to make better use of scarce AI experience (41% versus 32%). Perhaps because successful AI initiatives are providing the money (through either cost savings or enhanced revenue) for a bigger hiring budget, they’re also more likely to be actively recruiting more AI specific talent (42% versus 32%). Finally, they’re also nearly one and a half times more likely than others (44% versus 30%) to plan on leveraging more third-party vendors, such as [**managed services providers**](https://www.pwc.com/us/en/services/managed-services.html) with their scalable and multifaceted AI workforce, for experience. What companies can do **Do more with less with AI.** The highest-value use of AI in the labor market today is to help people to do better work, reducing the pressure to fill hard-to-fill positions. That’s true both for routine tasks, which AI-backed automation can perform to save employees’ time, and for advanced, AI-specific roles. AI can, for example, often conduct even sophisticated data science tasks, helping compensate for the shortage of data scientists. **Make employees happier.** By reducing the need for rote work, AI can make employees’ work life easier and more engaging. By giving them the opportunity and training to work with cutting edge AI, you can help increase the value you’re providing them — as well as the value they can give you. AI can even help [**provide emotional support**](https://www.weforum.org/agenda/2021/07/here-s-how-artificial-intelligence-can-create-a-more-compassionate-workplace/) in the workplace, fighting productivity loss and burnout. **Invest in data-driven people. The fastest way to address the AI talent shortage is most often to take specialists who have some of the skills you need, then provide the rest. Consider teaching computer scientists data science, data scientists software engineering, statisticians AI-relevant data science, and business leaders a little of all of these fields. Besides filling talent gaps, this approach can enhance cooperation among the groups that AI requires.**

**DOD and Other Military bodies do have the incentive to create Super Soldiers- Research Shows**

**Palmquist & Lapham [ M. Steven Palmquist & Mary Ann Lapham, Software Institute Software programmers, 2013, DTIC. Parallel Worlds: Agile and Waterfall Differences and Similarities,** [**https://apps.dtic.mil/sti/pdfs/ADA610501.pdf**](https://apps.dtic.mil/sti/pdfs/ADA610501.pdf)**, 6/24/2022, MA]**

**One of the principles of evolutionary psychology states that adaptation is the act of making up for past shortfalls**. Therefore, it is only natural for military leaders to pursue new capabilities that will ensure their troops are more fit and prepared to respond to changes in national security strategy, and to operate in complex combat environments. **Rapid advancements in technology have changed the conduct of war.** Like the introduction of the spear and shield in ancient societies, the invention of the tank, aircraft and combat ships have shaped the warfare tactics of modern societies.59 D**efense officials have witnessed the effects of growing innovations in technology and the enemy’s application of its use on the battlefield**. Improvised explosive devices (IEDs) and explosively formed penetrators (EFPs) activated by long range cellular transmitters came as a surprise to forces entering Iraq and Afghanistan. As a result, the military has changed its strategy, tactics, and technology to stay abreast of the changing operating picture and the nuances of asymmetric conflict. Diminishing conservative strategies along with the continued development of more sophisticated enemy operations had triggered a phase of transformation within the DoD to create a more dynamic force to maintain battlefield superiority and information dominance. **An example is the employment of autonomous weapon systems like** t**he MQ-9 Reaper UAV that can gather intelligence through surveillance technologies, independently select and discriminate targets, and render lethal effects with minimal collateral damage.** Though technology continues to evolve and increase the lethality of today’s battlefield, it is unimaginable to think that these technologies will ever replace the human factor of warfare. The diverse nature of current combat operations has heightened awareness of the continued importance of the individual soldier. **The soldier and his team have always been the most critical integrated combat system and like the UAV, these assets require optimization to increase performance and promote their effectiveness and lethality of the battlefield. The military found that the best way to defeat this asymmetric threat it to employ small groups of elite soldiers who are physically and mentally fit to withstand the rigors of war.** The surge during the Bush administration called for over 92,000 troops to conduct counterinsurgency operations in Iraq. To achieve the mandated quota, standards for recruitment were lowered, resulting in a force that was very clearly substandard with regard to IQ and physical prowess.60 Statistics released by the National Priorities Project provide a closer look at some very disheartening data on the quality of U.S. military recruits. The report shows that in 2007 only 70 percent of the population of military recruits had a high school diploma, which is significantly lower than the traditional accession goal of 96.8 percent and a decline not seen since WWII and Vietnam. In the same year, based on Armed Forces Qualification Test (AFQT) scores only 44.9 percent of recruits were categorized as high quality, which was an 11 percent decrease from 2005. Another grim detail highlighted in the report shows that the military increased their minimum percentage recruitment standard for personnel falling within the “Category IV” aptitude range to .4 percent. Soldiers that fall within this category are considered below average trainability and past DoD policy restricted Category IV enlistment to no more than .2 percent. **On a good note, despite not yet meeting prescribed objectives, the quality of soldiers within the armed forces is steadily progressing.61 An article by journalist Fred Kaplan states that “a dumber army is a weaker army” and in the era of persistent asymmetric conflict soldier are required to be stronger and more intelligent to overcome the obstacle imposed by this type of warfare.**62 This data does not intend to label the military as an institution of idiots rather it shows that in times of increased operational need the organization may not get the caliber of personnel it requires. **In a technical report released in 2003 by Strategic Analysis, Inc., officials from the DARPA state that the Peak Soldier Performance** (PSP) program was: …designed with the vision of enhancing warfighters’ physiological abilities and providing them the stamina, strength, and **endurance needed to complete grueling extended military operations**. **The mission of the warfighter is limited by his/her ability to sustain physical and cognitive performance** over extended periods of time and in extreme environments. At present, the warfighter does not possess the physiological and psychological capabilities to keep up with the advances in technology.63 The 2010 Defense Quadrennial Review Report, **the Department of Defense (DoD) also asserted its need to focus on evolving and enhancing the force in order to protect and advance U.S. interests in the near and long term future while remaining capable of conducting full spectrum operations unilaterally or in partnership with allied forces**.64 In order to create a more dynamic force to remain superior over its adversaries**, the DoD has expanded its interests in the study of biotechnological enhancement to include continued DNA research, studies in genetic engineering, a**nd continued research of the human metabolic process to develop better performance enhancing supplements for increased energy and endurance. While the programs are still in their infancy, ongoing research continues to unlock genetic codes, moving researchers closer to their desired goal of creating the “super soldier.” **The conceptual super soldier is one who is more decisive, protected, and equipped to survive the battlefield. Their bodies will quickly adjust to extreme temperatures, while increased tissue regeneration will promote the rapid wound healing and recovery.** Soldiers will be able to detect adverse situations and quickly traverse complex targets via their optimized ability to solve problems. Heightened endurance and lessened fatigue will ensure unit success during extended combat operations. The idea is simple: whether a threat is conventional or complex, **the soldier that possesses more superior physiological and mental capabilities than his enemy will prevail**.65 Therefore, we must explore the possible benefits of genetic engineering because it could potentially lessen the innate limitations of the American soldier bringing them to parity with other decisive large platform weapon systems.

## TEVV

### 1NC --- TEVV

#### Investing in Effective TEVV solidifies US leadership on AI – it sets a norm for other nations and private companies

**Flournoy, Haines et al 2020 - former Under Secretary of Defense for Policy and Director of National Intelligence** [Michèle and Avril, Gabrielle Cheftiz Special Assistant to the Under Secretary of Defense for Policy October, “Building Trust through Testing Adapting DOD’s Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems” https://cset. georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf Acc 6/23/22 JZ]

Third, with an effective TEVV system, the United States can reduce barriers to innovation and facilitate U.S. leadership in ML/DL technologies. As most of the innovation in ML/DL will come from the private sector, unless the U.S. government is able to effectively draw on private sector work in this arena, it will not be able to leverage the best cutting-edge technology. Research on new TEVV methods and organizational reforms to adapt the current system is simply not keeping pace with private sector development. Without urgent reforms and prioritized investment in new research and infrastructure, the Defense Department will lose its chance to shape industry’s approach to ML/DL development in a manner consistent with DOD standards for safety, reliability, and accountability. It will lose the opportunity to take advantage of new private sector developments, while allowing other nations without such standards to adopt the latest innovations. It is critical that the U.S. government not only shape its own U.S. industry standards but also promote compatible global standards and norms.

### 2NC --- TEVV Solves

#### TEVV is key to effective deployment of AI – it is necessary to build trust in commanders and operators. Broken weapons don’t improve our readiness

**Flournoy, Haines et al 2020 - former Under Secretary of Defense for Policy and Director of National Intelligence** [Michèle and Avril, Gabrielle Cheftiz Special Assistant to the Under Secretary of Defense for Policy October, “Building Trust through Testing Adapting DOD’s Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems” https://cset. georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf Acc 6/23/22 JZ]

The Pentagon cannot let TEVV become a barrier to fielding AI-enabled systems in an operationally relevant time frame, but must do so in a manner that engenders trust in such systems and is consistent with U.S. values and principles. The ultimate goal of any TEVV system 4 should be to build trust—with a commander who is responsible for deploying a system and an operator who will decide whether to delegate a task to such system—by providing relevant, easily understandable data to inform decision-making. Fielding AI systems before our competitors may not matter if DOD systems are brittle and break in an operational environment, are easily manipulated, or operators consequently lose faith in them. Military operations present a challenging environment. The Defense Department needs ML/DL systems that are robust and secure. They need to be able to function in a range of environmental conditions, against adversaries who are adaptive and clever, and in a manner that engenders trust by the warfighter.

#### TEVV is key to protect military AI from cyber attacks – AI systems are prone to attack and failure – TEVV helps promote innovations to prevent these attacks.

**Flournoy, Haines et al 2020 - former Under Secretary of Defense for Policy and Director of National Intelligence** [Michèle and Avril, Gabrielle Cheftiz Special Assistant to the Under Secretary of Defense for Policy October, “Building Trust through Testing Adapting DOD’s Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems” https://cset. georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf Acc 6/23/22 JZ]

Second, the context in which DOD operates means these technologies are prone to adversary attack and system failure, with very real consequences. Machine learning systems have an increased potential for failure modes relative to other systems, such as bias due to a distribution shift in data, as well as novel vulnerabilities to attacks ranging from data poisoning to adversarial attacks. One could easily imagine an image classifier that accidentally classifies a civilian school bus as a tank or an adversary exfiltrating a model processing sensitive intelligence, surveillance, and reconnaissance or communications data. Image classification algorithms developed for one environment (e.g., the desert) could turn out to work incorrectly in another environment (e.g., cities).

Third, with an effective TEVV system, the United States can reduce barriers to innovation and facilitate U.S. leadership in ML/DL technologies. As most of the innovation in ML/DL will come from the private sector, unless the U.S. government is able to effectively draw on private sector work in this arena, it will not be able to leverage the best cutting-edge technology. Research on new TEVV methods and organizational reforms to adapt the current system is simply not keeping pace with private sector development. Without urgent reforms and prioritized investment in new research and infrastructure, the Defense Department will lose its chance to shape industry’s approach to ML/DL development in a manner consistent with DOD standards for safety, reliability, and accountability. It will lose the opportunity to take advantage of new private sector developments, while allowing other nations without such standards to adopt the latest innovations. It is critical that the U.S. government not only shape its own U.S. industry standards but also promote compatible global standards and norms.

Fourth, adversary advancements will likely increase pressure to field AI-enabled systems faster, even if testing and assurance are lacking. China has elevated AI to be a major national priority across sectors and is already exporting armed drones with varying degrees of autonomy.3 Russia is also pursuing R&D on AI for military 5 purposes4 and fields AI-enabled robotic systems in Syria with little regard for ethical considerations.5 However, it shouldn’t be a race against our competitors to field AI systems at any cost. It’s a race to field robust, lawful, and secure AI systems that can be trusted to perform as intended.

Finally, high standards for robustness, assurance, interpretability, and governability can ultimately be a tremendous source of strategic advantage, incentivizing industry to harden systems to adversary attack. Taken together, these risks and opportunities suggest that devising an effective, efficient, and ethical TEVV process is critical for maintaining the U.S. military and economic competitive edge, as well as deploying reliable and trustworthy ML/DL systems.

### 2NC --- DOD fails

#### DOD has not committed to improve TEVV – this prevents the US from adopting safe AI

**Flournoy, Haines et al 2020 - former Under Secretary of Defense for Policy and Director of National Intelligence** [Michèle and Avril, Gabrielle Cheftiz Special Assistant to the Under Secretary of Defense for Policy October, “Building Trust through Testing Adapting DOD’s Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems” https://cset. georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf Acc 6/23/22 JZ]

The Defense Department needs to reform its existing testing and verification system—its methods, processes, infrastructure, and workforce—in order to help decision-makers and operators understand and manage the risks of developing, producing, operating, and sustaining AI-enabled systems. Several DOD reports and policy documents identify TEVV as a barrier to AI adoption and call for increased research into new methodologies, including the Pentagon’s AI Ethics Principles1 and AI Strategy,2 which states, “we will invest in the research and development of AI systems that are resilient, robust, reliable, and secure; we will continue to fund research into techniques that produce more explainable AI; and we will pioneer approaches for AI test, evaluation, verification, and validation.” However, DOD has yet to translate this stated goal into a real plan of action. Advancing the Defense Department’s TEVV enterprise for ML/DL systems is critical for several reasons. First, developing an effective TEVV approach that is sufficiently predictive of performance is critical to building the trust in these systems necessary to deploy and leverage these capabilities at scale. The United States has already seen this dynamic with nuclear power, for example, where lost trust in the technology has prevented policymakers from harnessing nuclear power for clean energy

**Alternate Causality - Limited DOD data prevent testing and verification of AI**

**Flournoy, Haines et al 2020 - former Under Secretary of Defense for Policy and Director of National Intelligence** [Michèle and Avril, Gabrielle Cheftiz Special Assistant to the Under Secretary of Defense for Policy October, “Building Trust through Testing Adapting DOD’s Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems” https://cset. georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf Acc 6/23/22 JZ]

Testing ML/DL requires large, representative data sets. While technological advances in “one shot” and reinforcement learning may ultimately enable the Pentagon to test ML/DL without a lot of data or provide alternative approaches to handle out-of-distribution situations, for the next five to 10 years, the Defense Department will likely rely on supervised learning systems, and testing ML/DL systems will likely require large sets of labeled, representative data. The United States needs a whole-of-government data strategy that allows for data collection, cleaning, curation, and sharing across agencies, especially between DOD and the IC. Currently, the Defense Department lacks sufficient available data that mimics the conflict condition in which these systems may operate in the future. This will limit its ability to test system performance against realistic conditions. It will also hamstring efforts to identify edge cases and develop fail-safe mechanisms to prevent catastrophic outcomes. The Pentagon lacks the ability to effectively collect, manage, store, and share testing data across the enterprise, which would enable this approach to scale. Finally, DOD leadership will need approaches to continuously test the quality of the data itself, as testing data could be compromised or revealed unintentionally or intentionally by adversaries. ML/DL will be integrated into a system of systems. ML/DL will be integrated into a range of DOD software and hardware systems, so it is imperative that developers, testers, and policymakers take a systems architecture view when building and evaluating these systems. The Defense Department cannot simply test all components separately and assume that the system as a whole will work as intended. The accuracy and precision of ML/DL systems is typically a composite effect that arises from a combination of the behaviors of different components, such as the training data, the learning program, and even the learning framework. These components are then embedded in larger systems, so interactions with the physical, computational, and human components of the system will ultimately affect system performance. Often, failures come from unexpected interactions or relationships between systems, rather than the behavior of any individual element. These dynamics make the system increasingly vulnerable to malfunction and cyber-attacks. An adversary could attack any number of vulnerable entry points within the hardware or software that could, in turn, compromise the entire system.11 The Defense Department needs to greatly advance its ability to conduct integrated systems testing that takes into account the interactions with and between systems, testing both machine-machine and human-machine interactions. It should also prioritize testing for how failure in a given subsystem could impact the performance of the system as a whole.

## Misc

### 2NC --- No Solvency AI

#### No solvency – the DoD is too incompetent to be put in charge of AI development

McCord 21 (Mark, “China Already Outflanks US in AI, Says Ex-Pentagon Tech Chief,” Asia Financial, https://www.asiafinancial.com/china-already-outflanks-us-in-ai-says-ex-pentagon-tech-chief)

China is set for global dominance of the artificial intelligence space, the Pentagon’s recently resigned first chief of software officer has said, adding that he stepped down because the US had been too slow to develop the technology. Nicolas Chaillan, a technology entrepreneur, left the Department of Defence in October 2021 after spending three years trying to develop cyber security systems with the US Air Force. But he told the Financial Times that he resigned because he couldn’t bear to watch the US flounder on AI. “We have no competing fighting chance against China in 15 to 20 years,” he was quoted as telling the UK-based newspaper. “Right now, it’s already a done deal; it is already over in my opinion.” The 37-year old said he was “angry” at the pace of development in the US, arguing that AI was more vital to US interests than military hardware. A congressionally mandated national security commission offered similar warnings of China’s imminent AI supremacy earlier this year. Part of the problem, Chaillan told the FT, was that Google had been reluctant to work with the Defence department on the technology. And in his resignation letter, Chaillan said military personnel had been put in charge of cyber security when they had none of the skills required to tackle it. “[W]e are setting up critical infrastructure to fail,” he wrote. “We would not put a pilot in the cockpit without extensive flight training; why would we expect someone with no IT experience to be close to successful? While we wasted time in bureaucracy, our adversaries moved further ahead.” Consequently, cyber defences in some government departments were at “kindergarten levels”, he was quoted as saying.

### 2NC --- SpaceX solves AI

#### SpaceX has autonomous Spaceships now – it can implement the plan

Neel V. Patel, 7-3-2020, "Are we making spacecraft too autonomous?," MIT Technology Review, https://www.technologyreview.com/2020/07/03/1004788/spacecraft-spacefight-autonomous-software-ai/

When SpaceX’s Crew Dragon took NASA astronauts to the ISS near the end of May, the launch brought back a familiar sight. For the first time since the space shuttle was retired, American rockets were launching from American soil to take Americans into space.

Inside the vehicle, however, things couldn’t have looked more different. Gone was the sprawling dashboard of lights and switches and knobs that once dominated the space shuttle’s interior. All of it was replaced with a futuristic console of multiple large touch screens that cycle through a variety of displays. Behind those screens, the vehicle is run by software that’s designed to get into space and navigate to the space station completely autonomously.

“Growing up as a pilot, my whole career, having a certain way to control a vehicle—this is certainly different,” Doug Hurley told NASA TV viewers shortly before the SpaceX mission. Instead of calling for a hand on the control stick, navigation is now a series of predetermined inputs. The SpaceX astronauts may still be involved in decision-making at critical junctures, but much of that function has moved out of their hands.

Does this matter? Software has never played a more critical role in spaceflight. It has made it safer and more efficient, allowing a spacecraft to automatically adjust to changing conditions. According to Darrel Raines, a NASA engineer leading software development for the Orion deep space capsule, autonomy is particularly key for areas of “critical response time”—like the ascent of a rocket after liftoff, when a problem might require initiating an abort sequence in just a matter of seconds. Or in instances where the crew might be incapacitated for some reason.

And increased autonomy is practically essential to making some forms of spaceflight even work. Ad Astra is a Houston-based company that’s looking to make plasma rocket propulsion technology viable. The experimental engine uses plasma made out of argon gas, which is heated using electromagnetic waves. A “tuning” process overseen by the system’s software automatically figures out the optimal frequencies for this heating. The engine comes to full power in just a few milliseconds. “There’s no way for a human to respond to something like that in time,” says CEO Franklin Chang Díaz, a former astronaut who flew on several space shuttle missions from 1986 to 2002. Algorithms in the control system are used to recognize changing conditions in the rocket as it’s moving through the startup sequence—and act accordingly. “We wouldn’t be able to do any of this well without software,” he says.

But overrelying on software and autonomous systems in spaceflight creates new opportunities for problems to arise. That’s especially a concern for many of the space industry’s new contenders, who aren’t necessarily used to the kind of aggressive and comprehensive testing needed to weed out problems in software and are still trying to strike a good balance between automation and manual control.

space shuttle Atlantis

The Space Shuttle Atlantis had a more traditional dashboard for its pilots to utilize.

inflight video of Dragon 2 mission

The Crew Dragon capsule replaces the knobs and switches with large touchscreens.

Nowadays, a few errors in over one million lines of code could spell the difference between mission success and mission failure. We saw that late last year, when Boeing’s Starliner capsule (the other vehicle NASA is counting on to send American astronauts into space) failed to make it to the ISS because of a glitch in its internal timer. A human pilot could have overridden the glitch that ended up burning Starliner’s thrusters prematurely. NASA administrator Jim Bridenstine remarked soon after Starliner’s problems arose: “Had we had an astronaut on board, we very well may be at the International Space Station right now.”

But it was later revealed that many other errors in the software had not been caught before launch, including one that could have led to the destruction of the spacecraft. And that was something human crew members could easily have overridden.

Boeing is certainly no stranger to building and testing spaceflight technologies, so it was a surprise to see the company fail to catch these problems before the Starliner test flight. “Software defects, particularly in complex spacecraft code, are not unexpected,” NASA said when the second glitch was made public. “However, there were numerous instances where the Boeing software quality processes either should have or could have uncovered the defects.” Boeing declined a request for comment.

According to Luke Schreier, the vice president and general manager of aerospace at NI (formerly National Instruments), problems in software are inevitable, whether in autonomous vehicles or in spacecraft. “That’s just life,” he says. The only real solution is to aggressively test ahead of time to find those issues and fix them: “You have to have a really rigorous software testing program to find those mistakes that will inevitably be there.”

Enter AI

Space, however, is a unique environment to test for. The conditions a spacecraft will encounter aren’t easy to emulate on the ground. While an autonomous vehicle can be taken out of the simulator and eased into lighter real-world conditions to refine the software little by little, you can’t really do the same thing for a launch vehicle. Launch, spaceflight, and a return to Earth are actions that either happen or they don’t—there is no “light” version.

This, says Schreier, is why AI is such a big deal in spaceflight nowadays—you can develop an autonomous system that is capable of anticipating those conditions, rather than requiring the conditions to be learned during a specific simulation. “You couldn’t possibly simulate on your own all the corner cases of the new hardware you’re designing,” he says.

So for some groups, testing software isn’t just a matter of finding and fixing errors in the code; it’s also a way to train AI-driven software. Take Virgin Orbit, for example, which recently tried to send its LauncherOne vehicle into space for the first time. The company worked with NI to develop a test bench that looped together all the vehicle’s sensors and avionics with the software meant to run a mission into orbit (down to the exact length of wiring used within the vehicle). By the time LauncherOne was ready to fly, it believed it had already been in space thousands of times thanks to the testing, and it had already faced many different kinds of scenarios.

Of course, the LauncherOne’s first test flight ended in failure, for reasons that have still not been disclosed. If it was due to software limitations, the attempt is yet another sign there’s a limit to how much an AI can be trained to face real-world conditions.

Raines adds that in contrast to the slower approach NASA takes for testing, private companies are able to move much more rapidly. For some, like SpaceX, this works out well. For others, like Boeing, it can lead to some surprising hiccups.

Ultimately, “the worst thing you can do is make something fully manual or fully autonomous,” says Nathan Uitenbroek, another NASA engineer working on Orion’s software development. Humans have to be able to intervene if the software is glitching up or if the computer’s memory is destroyed by an unanticipated event (like a blast of cosmic rays). But they also rely on the software to inform them when other problems arise.

NASA is used to figuring out this balance, and it has redundancy built into its crewed vehicles. The space shuttle operated on multiple computers using the same software, and if one had a problem, the others could take over. A separate computer ran on entirely different software, so it could take over the entire spacecraft if a systemic glitch was affecting the others. Raines and Uitenbroek say the same redundancy is used on Orion, which also includes a layer of automatic function that bypasses the software entirely for critical functions like parachute release.

On the Crew Dragon, there are instances where astronauts can manually initiate abort sequences, and where they can override software on the basis of new inputs. But the design of these vehicles means it’s more difficult now for the human to take complete control. The touch-screen console is still tied to the spacecraft’s software, and you can’t just bypass it entirely when you want to take over the spacecraft, even in an emergency.

There’s no consensus on how much further the human role in spaceflight will—or should—shrink. Uitenbroek thinks trying to develop software that can account for every possible contingency is simply impractical, especially when you have deadlines to make.

Chang Díaz disagrees, saying the world is shifting “to a point where eventually the human is going to be taken out of the equation.”

Which approach wins out may depend on the level of success achieved by the different parties sending people into space. NASA has no intention of taking humans out of the equation, but if commercial

# Cyber

## 5-G

### 1NC --- 5-G

#### CP solves and avoids the net benefit – The US CAN unilaterally overtake China in the 5G race

**Brake and Bauer 20** [Doug Brake – Former Director, Broadband and Spectrum Policy, Information Technology and Innovation Foundation, and Alexandra Bauer, Policy Analyst, Information Technology and Innovation Foundation" The Great 5G Race: Is China Really Beating the United States?" ITIF, https://itif.org/publications/2020/11/30/great-5g-race-china-really-beating-united-states/] Blitz

**INTRODUCTION** 5G is expected to provide the connective tissue for many emerging technologies critical to productivity, innovation, and national competitiveness. Some commentators have panicked over the so-called “race” for 5G, pointing in fear at China’s hundreds of thousands of new base stations, and projections of hundreds of millions of 5G subscribers this year alone. But if we are going to base policy decisions on this race (and it is questionable that we should), understanding how infrastructure and subscription numbers are actually counted matters. A closer look reveals that China’s wireless infrastructure and subscriber numbers are not as impressive as they may first appear: By counting anyone on a 5G plan—even if they only have a 4G device connecting to 4G infrastructure—as a 5G subscriber, and measuring individual base stations instead of cell sites, China’s 5G stats can paint a misleading picture. This misleading picture leads to the interpretation that the sky is falling. **THE SKY IS FALLING: CLAIMS THAT CHINA IS BEATING THE UNITED STATES AT 5G** One can barely scan a technology news site without reading that the United States is losing to China in 5G, and that this will mean economic catastrophe. Headlines such as “China’s Dominance Of 5G Networks Puts U.S. Economic Future At Stake” and “China’s growing 5G dominance is a disaster for US security” keep policymakers on edge when considering how the United States should move forward with the next generation of wireless.1 The fear is that the first country to build 5G networks will have a head start in developing the emerging technologies that depend on 5G’s low-latency, high-throughput wireless connectivity. As Attorney General William Barr put it, “China’s success in 5G infrastructure is also translating into advantages in a range of new technologies associated with 5G.”2 He claimed, “Within the next five years, 5G global territory and application dominance will be determined,” and “the stakes for the United States could not be higher.”3 Are these Chicken Littles to be believed? Certainly, China has advantages in deploying 5G infrastructure, with state-directed companies making investments that market actors might not. But it is important we have a strong understanding of the metrics of Chinese 5G deployment, and the methodology for counting before calling the 5G race. **5G USERS VERSUS SUBSCRIBERS** Many reports likely overstate the extent of Chinese 5G deployment for several reasons. Part of this is likely due to intentional inflation of statistics reported by operators under pressure from Chinese authorities. This is a long-standing practice in China, going back at least as far as Mao and agricultural communes reporting fake crop yields so as not to displease leadership.4 And today they are not unique to the telecom sector, as organizations of all kinds inflate numbers in order to meet Beijing’s expectations. The Ministry of Industry and Information Technology (MIIT) put out a statement encouraging telecommunications providers to “accelerate user migration to 5G through measures such as package upgrade offer, and credit purchases, etc.”5 Providers then started encouraging or even forcing customers to upgrade to 5G subscriptions regardless of their actual need, use, or device.6 Some companies reduced 5G subscription prices so much they are even cheaper than staying on a 4G plan.7 As one reporter put it, “[W]ith all of China’s big telcos slashing 5G package prices in the past few months, it could well be that customers are being drawn in more by attractive tariffs than by a desire to get their hands on the latest hardware and its related capabilities.”8 The push for 5G subscribers was evident before 5G was even activated: Although 5G service was not turned on in China until November of 2019, Chinese telecom providers listed 9 million 5G users in October 2019, a month prior to its actual activation.9 By counting anyone on a 5G plan—even if they only have a 4G device connecting to 4G infrastructure—as a 5G subscriber, and measuring individual base stations instead of cell sites, China’s 5G stats paint a misleading picture. Apparently, the numbers game went too far, as the MIIT later called upon providers to “clean up” reporting and end aggressive sales practices after news of subscriber inflation spread.10 But current numbers are still plagued with confusion. Consider that China Telecom and China Mobile (the two largest operators in China) reported 150 million “5G package customers” as of September 2020. But according to China’s Academy for Information and Communications Technology, only 94 million 5G devices had been shipped for all of China during the same time frame, indicating a sizable gap between the number of “subscribers” and actual 5G users.11 The discrepancy may be due largely to terminology: “5G package customers” is a blanket term often used by Chinese carriers to refer to anyone on a 5G subscription, regardless of whether they actually have a 5G device or access to a 5G network.12 China Mobile acknowledges that they count anyone “who has subscribed to 5G tariff plans” as a 5G customer.13 The number of 5G-capable devices alone is impressive, and the competitive threat from China justifies a thoughtful policy response, but no one should be worked into a panic by goosed stats. **NETWORK DEPLOYMENT: BASE STATIONS VERSUS CELL SITES** Subscriptions are not the only potentially misunderstood stat. Chinese operators tend to count mobile infrastructure differently from how Western operators generally do. The key difference is between cell sites (how U.S. telecommunications operators typically measure deployment) and base stations (how Chinese telecommunications operators typically measure deployment). A cell site usually refers to the entire area of a given tower, which includes potentially multiple base stations and antennas using different spectrum. The term “base station” generally refers to the equipment each carrier uses to send signals over multiple antennas at the cell site. Often one cell site will have multiple base stations, sometimes it will host only one. But generally, it is not a one-to-one conversion between base stations and cell sites or towers; It is important that these numbers are not conflated to mean the same thing. Deployment figures are often further mischaracterized because of the way Chinese operators sometimes count each spectrum band as a separate “logical” base station instead of actual pieces of equipment.14 Just like how a Wi-Fi router can work on different spectrum (generally 2.4 GHz and 5 GHz), a mobile base station can operate on multiple spectrum bands. American carriers would generally count a multi-spectrum base station as at most one piece of equipment. But some Chinese reporting apparently treats each individual spectrum band a base station supports as a different “logical site.”15 A representative from Huawei explained that “a China Unicom base station supports GSM 900, GSM 1800, WCDMA 2100 and LTE. Most of the equipment is deployed in the same room at one physical site, but there are four bands, so there are four logical sites.”16 As a result, Chinese numbers could easily be misrepresented as three to four times higher compared with how Western operators tend to count equipment.17 Policymakers and the media should take care not to conflate estimates of base stations for logical sites with actual, physical cell sites—these are two totally different measurements. For a rough comparison, it seems fair to assume two or three base stations per cell site, but the number of logical sites—meaning each spectrum band used—could be many more. **ACTUAL PERFORMANCE** The raw number of base stations is not always a good measure of a network’s performance. What we really care about is a network’s performance for the population it covers. Measuring performance becomes increasingly complicated with 5G’s diverse spectrum assets, some of which do not use the traditional cellular architecture. The utilization of different spectrum resources or amounts of bandwidth results in varying levels of performance even with equal levels of infrastructure. This is relevant when comparing China, which so far uses exclusively mid-band spectrum for 5G, with the United States, which has made a large push to focus on high-band coverage. High-band 5G offers the highest performance leap over existing networks, at least where it is available. But that being said, let’s try a rough comparison, assuming the similar spectrum assets and using China’s announcement that it anticipates 600,000 5G base stations by the end of 2020.18 Assume three base stations per Chinese cell site—one for each of the major operators—and we get about 200,000 sites. This could be several times lower if we’re talking logical sites, but it is hard to say—let’s keep the estimate conservative and set that issue aside. The population served also plays a big role in the performance of a given network. China’s population is about 1.39 billion. This is about 4.5 times larger than that of the United States, indicating Chinese operators will need roughly 4.5 times as many base stations as their U.S. counterparts to get a similar level of performance for each user (all else being equal). So, those 200,000 sites work out to about 1 site per 7,000 people. In 2019 alone, U.S. operators invested in 5G-ready cell sites and added 46,000 new cell sites—roughly 1 site per 7,134 people.19 To the uninformed, 600,000 base stations might sound alarming, but understanding what those numbers mean, we’re about neck-and-neck. If we assume that the Chinese sites include logical sites, and the spectral efficiency of their base stations is less, then it appears the United States is clearly in the lead. Slow and steady may win the race. Whereas the United States is pursuing a gradual, economical deployment of 5G, the problems with China’s rushed 5G deployments are already starting to show. One of Huawei’s own executives went so far as to call China’s 5G “fake, dumb and poor,” mostly due to poor integration with the 4G network.21 Another former official warned in a recent speech that China’s 5G push could become a failed investment.22 While China is no doubt investing substantially in the expansion of its 5G network, including by pressuring its state-owned carriers to invest faster than the market demands, Chinese figures must be properly scrutinized when using them to make U.S. policy decisions.

### 2NC --- Solves China

#### Domestic investment solves the race against China for 5G

Peterson 18 - [Erik R. Peterson, 2018, "5G is the key to future American competitiveness," Germany, <https://www.de.kearney.com/business-policy/article/-/insights/5g-is-the-key-to-future-american-competitiveness>]//MLee

The telecom industry’s race for 5G is one of the most intense and consequential technological contests of our time. What will it take to win? As the global race to develop and deploy 5G telecommunications networks heats up, the urgency for American investment in its digital infrastructure is rising in tandem. Rapid and large-scale deployment of 5G would not only help the United States maintain its economic and technological edge globally, but it would also offer an opportunity to realize three other national objectives. First, it would support the transition of the economy to the Fourth Industrial Revolution ushered in by dramatic technology innovations. Second, it would promote a stronger, more innovative, and more competitive business landscape, which in turn would support sustainable and high-paying jobs. Finally, it would provide increased access, benefiting both local communities and the private sector in under-served areas. The stakes are extraordinarily high. The first country to achieve large-scale, reliable 5G coverage stands to reap significant economic gains—starting with higher technological innovation, elevated economic growth, and strengthened national competitiveness. The returns will be far larger than upfront investments. 5G: a world of change A new era of the digital economy was unleashed as wireless networks evolved from voice-only 2G, to voice and text, and then to the latest Internet-enabled 4G LTE technology. Once fully deployed, 5G will be similarly transformative, given its ability to support massive Machine to Machine (M2M) communications through greater bandwidth, such as between cellphones, sensors, “smart” machinery and appliances, and other Internet of Things (IoT) devices. In addition to IoT, 5G will support a range of new and future applications in each of the other next-generation technologies at the core of the [future of production](https://www.atkearney.com/operations-performance-transformation/article/-/insights/readiness-for-the-future-of-production-report-2018)—artificial intelligence, robotics, additive manufacturing, and augmented and virtual reality (AR/VR). There is no doubt that 5G will have a significant impact on American consumers. One obvious way will be from performance improvement, such as faster video streaming and real-time gaming thanks to the reduced latency provided by 5G networks. Kearney’s recent [Health@250](https://www.atkearney.com/web/health250/executive-summary) report highlighted how mobile health solutions from wearables, IoT devices, and related technologies will take advantage of 5G for improved data collection and real-time monitoring, while other advances such as remote surgery will also become possible. The power and convenience of 5G may even contribute to the next wave of “cord cutting” in fixed services—particularly given 5G's potential as a way to provide high-speed connectivity to customers currently underserved by existing fixed broadband infrastructure. Process innovation: an essential ingredient of competitive advantage Companies and their R&D arms are rethinking the way they manufacture both old and new products. In today’s hyper-competitive world, are you exploring every opportunity to innovate? 5G will also have a significant impact on the B2B market. The entire ICT industry—from chipmakers to telecom companies to hardware and software manufacturers—is building out this technology with B2B customers and “things” top of mind. Businesses will have countless devices talking to one another as well as to the cloud, streaming massive amounts of data. While IoT devices are already proliferating rapidly due to the connectivity offered by today’s LTE networks, 5G will further enhance connectivity for these devices due to network slicing, improved spectrum efficiency, and better power management. As a result, businesses will be able to better manage fields and factories with much lower latency than is possible with current WLAN networks, track goods in real time along their supply chains, and follow products from the retail shelf into the home. Data sharing will also be multidirectional. For instance, a truck tire will simultaneously collect data on wear and tear, road conditions, temperature, and air pressure for both the vehicle owner and the tire manufacturer, providing crucial inputs for maintenance schedules and future product development. Finally, take “[smart cities](https://www.atkearney.com/global-cities/full-report),” which promise better traffic management, improved car safety, and route optimization. What makes them “smart” is the ability of their systems to share large amounts of data instantly between other cars, road sensors, traffic lights, and other devices. And while there is always a trade-off between supporting M2M and latency in any network, 5G will see improvements in both, leading to significantly improved performance across the spectrum of 5G use cases. According to Rob Thies, general partner at World Innovation Lab Ventures, “5G is as big as the transition from dial-up to DSL, and will change the world just as much.” [Qualcomm estimates](https://qualcomm.com/invention/5g/economy) that the global 5G value chain will be $3.5 trillion by 2035, which is larger than the entire mobile value chain today. Add to that another $12.3 trillion in “5G-enabled” growth. For the United States, the projected economic impact is no less staggering. The telecommunications industry association CTIA estimates that 5G will create three million new jobs, on top of a wireless industry that already supports 4.7 million workers. It will also generate an estimated $500 billion in economic growth—including 5G-enabled innovation by startups and major companies alike that will add new economic value. The efficiency and speed with which 5G delivers these economic and social benefits, however, will depend on the scale, timeline, and geographic scope of the investments made by the mobile operators, as well as how friendly government policies are to 5G adoption, including wireless spectrum auction processes. Importantly, 5G opens up enormous new blocks of spectrum, making it most cost-effective to serve the relentless rise in traffic on networks. What are the incentives for 5G? A key incentive for making such an investment is the potential for new revenue streams, accomplished in part by working more closely with B2B companies. For example, given the significant B2B market for 5G capabilities, it is likely that changes will occur in the cost structures for what are known as “over-the-top,” or OTT, services such as current video content providers and future AR/VR services and autonomous vehicle operators, as well as their relationships with telecom companies. For example, Tesla is [partnering with Intel](https://teslanomics.co/tesla-model-3-and-others-will-uses-intel-for-5g/) to bring 5G connectivity to its vehicles. Further, Ericsson estimates the potential market size for industry digitalization that telecoms could tap into will be nearly $620 billion by 2026. We therefore expect to see considerable experimentation and innovation in this space in the coming years. B2C will also provide incentives for investment in 5G, particularly as mobile use continues to rise globally. As reinforced by the Mary Meeker’s [2018 Internet trends report](https://www.recode.net/2018/5/30/17385116/mary-meeker-slides-internet-trends-code-conference-2018), mobile Internet usage remains the key driver of digital media consumption. Global average smartphone costs continue to decline, mobile payments are increasingly standard, and the mobile experience is becoming further ingrained in people’s daily lives. With 5G, more services can be brought to mobile, further amplifying the scope for innovation. The global 5G race Major economies around the world—particularly those in Asia—are working aggressively to develop 5G networks. The Chinese government, for example, is [actively pushing](http://english.gov.cn/state_council/ministries/2017/10/02/content_281475896725312.htm) for 5G amid a broader effort to strengthen its digital economy, including through its “Made in China 2025” initiative. South Korea used the occasion of the 2018 Olympics to demonstrate its 5G prowess. A [drone connected to a 5G network](http://koreabizwire.com/in-two-firsts-drone-carries-olympic-torch-at-night-in-seoul-city-square/107542) even carried the Olympic torch. And Japan is expected to use the 2020 Olympic Games to do the same. Australia, the United Kingdom, and others will also test 5G networks in the coming months and years. CTIA forecasts that US telecoms will invest $275 billion in 5G technology, including fiber-optic cables, small cells, and other 5G network infrastructure. All the major US telecoms are planning 5G trials in 2018 and 2019 across dozens of cities—with 2020 as the consensus tipping point for 5G across major urban centers—fostered by strong competition among them to be the first to deliver 5G to customers. Indeed, a key stated goal of the [proposed merger between T-Mobile and Sprint](https://newtmobile.com/sparking-the-5g-economy/) is to utilize their combined assets to become the first nationwide 5G carrier. Such a development would push other telecoms to accelerate their 5G rollouts in order to compete in the marketplace, improving mobile access for consumers and businesses throughout the country. For their part, [AT&T](https://venturebeat.com/2018/05/16/att-were-ok-with-t-mobile-sprint-merger-planning-for-hyper-accurate-5g-gps-and-vr-parks/) and [Verizon](https://venturebeat.com/2018/05/03/verizon-pegs-2019-for-mobile-5g-as-sprint-seeks-millimeter-wave-spectrum/) have both discussed how 5G is creating new opportunities for all the top US telecoms, with each one implementing a different strategy to develop and deploy its capabilities. At the same time, the rollout of 5G will allow telecoms to retire some of the capacity dedicated to 2G and 3G networks, enabling important cost savings and reinvestment of resources, as well. US telecoms may also use the deployment of 5G to capture a previously untapped and underserved customer base—rural America. In this effort, public and private sector interests would be aligned. The US Federal Communications Commission has identified 5G investment as integral to [closing the digital divide](https://www.publicintegrity.org/2018/03/02/21479/fcc-says-small-cells-will-close-digital-divide-most-say-they-wont) that still persists today. Opportunities may therefore emerge for public-private partnerships between telecoms and governments at the local, state, and federal levels to roll out 5G coverage, particularly to underserved areas. This is important, as concerns regarding the social impact of technology are growing, including whether the 4IR will reduce or exacerbate inequality. Such questions will in large part determine the long-term outlook for the United States, as explored in our [America@250](https://www.atkearney.com/web/america250/four-futures) effort to assess the outlook for the country our to its 250th anniversary in 2026 and beyond. What will it take to win the 5G race? The future center of global technological change will shift as a result of who wins the 5G race. To be sure, not every country is a perfect candidate for aggressive 5G investments given variations in market size, level of technological penetration, the size of the rural market, and other factors. Additionally, questions remain regarding the business case for large-scale 5G investments, as the average consumer [may yet be unwilling to pay a premium for low latency or high-speed connections](https://www.atkearney.com/documents/291362523/291366299/NextGen--Succeeding+with+the+Digital+Consumer.pdf/ca8639d9-fc3a-8769-7834-f824f500ce27?t=1519665205000). But national competitiveness, particularly for the world’s major economies, will increasingly be determined by the level of 4IR technological adoption and innovation, which in turn will depend on the quality of national 5G wireless networks. Winning the 5G race requires ensuring that coverage is both broad and deep across a given market. Only then will the impacts of massive infrastructure investments, job creation, and broader economic growth be realized. To upgrade its digital infrastructure quickly and efficiently, the United States must ensure that the proper incentives are in place to foster massive investments by—and healthy competition among—the country’s telecom companies. These companies also need the space to innovate and experiment with new business models in collaboration with the wide variety of industries expected to leverage 5G. America’s future competitiveness depends on it.

## NATO

### 1NC --- Cyber Task force

#### That solves cyber security/ critical infrastructure

Quested ‘22 - [Tony Quested, 6/15/22, "Darktrace CEO calls for ‘tech NATO’ to police cybercrime," business weekly, <https://www.businessweekly.co.uk/killer-50/50-insider/darktrace-ceo-calls-%E2%80%98tech-nato%E2%80%99-police-cybercrime>] //MLee

The CEO of Killer50 superstar Darktrace says there is “a shocking tolerance” to cyber attacks and urges additional vigilance. Poppy Gustafsson spoke at the Royal United Services Institute (RUSI) on the evolving cyber threat landscape in the context of Russia’s invasion of Ukraine. She was in conversation with Professor Madeline Carr, Senior RUSI Associate Fellow and Professor of Global Politics and Cybersecurity at University College London. Commenting on the challenge of policing both cyber warfare and international cyber crime, Gustafsson said “There remains a persistent lack of clarity around how we define an act of war in the cyber-sphere.” She called for the creation of a dedicated international cyber task force, or ‘tech NATO’, to deliver international collaboration in agreeing and ratifying a set of cyber-norms and accountability. Gustafsson noted that Russia’s invasion of Ukraine is the first time an active invasion has been supported by the tactical dismantling of national infrastructure using cyber-attacks. “The attack on the Viasat satellite that disabled Ukrainian military communications one hour before the invasion was a key component of the beginning of this war,” argued Gustafsson. She added: “We have seen UK, US and EU officials jointly attribute this attack to Russia, an immensely political act. That is unprecedented.” Asked by Prof. Carr whether Darktrace had seen the level of collateral cyber disruption it expected, Gustafsson shared that Darktrace data showed a global increase in attacks on critical national infrastructure bodies across its customer base, including a 90 per cent increase in high priority security incidents on the networks of energy companies in Europe during the week of the invasion, from February 24. At the domestic level, Gustafsson called for cooperation and accountability between the public and private sectors as well as lower tolerance for cyber attacks. She emphasised the importance of a “whole of society approach” to cyber security adding: “There is a shocking tolerance for cyber attacks, and that has to change. “Organizations that are custodians of valuable, private data cannot be allowed to let that data fall into criminal hands through negligence and face no consequences.” Professor Carr commented: “Issues that we had thought about speculatively have now become our reality. We are facing war in Europe and there is an essential cyber component both to the way it is being fought and to its international ramifications. What is needed is clarity, consensus and cooperation.” The Royal United Services Institute is the world’s oldest and the UK’s leading defence and security think tank. Darktrace has been a member since 2020.

### 1NC --- EU Hybrid Warfare

#### The CP solves through cooperating with the EU to stop Russian hybrid warfare against NATO.

**Chivvis 17** [Christopher S. Chivvis, a senior political scientist at the nonprofit, nonpartisan RAND Corporation and teaches at the Johns Hopkins School of Advanced International Studies, March 22, 2017, “Understanding Russian ‘Hybrid Warfare’”, RAND Corporation, <https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf>, JMH]

Developing Strategies to Counter Hybrid Warfare Meeting the challenge posed by Russian hybrid warfare will take time and effort. It must also be developed in conjunction with efforts to strengthen conventional deterrence. An effective strategy to defend U.S. interests against hybrid Russian strategies will include, at a minimum, the following. Support for transparency and anticorruption efforts. Tolerance of corruption greatly facilitates Russian influence strategies. Some countries in Europe—for example, many states in the Balkans—suffer from weak anticorruption legal frameworks and limited political will for change. In other countries, political will may be strong, but individual privacy concerns can limit the remit of transparency laws. **In these areas, the EU is an important partner for both the United States and for NATO. The United States should support European anticorruption efforts wholeheartedly, with appropriate funding for related State Department and U.S. Agency for International Development programs.** Support for internal security reform and defense institution building in targeted states such as the Balkans and Ukraine. Although some Balkan militaries already meet NATO standards of professionalization, others need additional support. **Institution-building in these countries needs to be focused on weakening any lingering ties with Russian security services**. In addition, **strengthening capabilities in such countries, as well as in the Baltic states, will enable greater detection and resistance to covert Russian operations.** In general, U.S. assistance targeted at strengthening the rule of law will complicate Moscow’s hybrid efforts.15 **Strategies to push back against Russian influence operations**. More work needs to be done in this difficult area, but initial research suggests that it may be better to focus on discrediting sources such as Russia Today and generally raising awareness of misinformation rather than attempting to fight each and every story on a tit-for-tat basis. **Civil society must also be encouraged to play a larger role in combatting Russian disinformation. Increasing the flow of positive information will also help**. In extreme cases, such as wartime, it may be necessary to temporarily close off access to Russian media outlets.16 Effective use of U.S. special operations forces in the U.S. European Command area of operations. U.S. special operations forces have an important role to play in combating Russian hybrid strategies in Europe. Both the mission and operating environment in Europe, however, is different from that in countries like Iraq and Syria. This requires some adaptation. For example, **one challenge is ensuring that U.S. diplomats are attuned to the needs of U.S. special operations forces conducting training and other activities in the region. Conversely, U.S. forces must also be fully aware of the delicate nature of some U.S. diplomatic activities underway in these same countries.** The United States must also operate in support of individual European countries’ plans, filling their gaps and bolstering their programs. Support for European efforts to combat Russian hybrid warfare. The United States, after all, is not the first line of defense against most forms of Russian hybrid warfare in Europe. Instead, the first line of defense is the EU and European countries themselves. The United States can support specific efforts, such as Finland’s Hybrid War Center of Excellence, Latvia’s Strategic Communications Center of Excellence, and Estonia’s Cyber Center of Excellence, while encouraging other best practices, such as closer public-private partnerships in Europe, to strengthen Europe’s own defenses against cyber attacks.

## Norms

### 1NC --- Norms

#### A norms-based approach is infinitely better – countries follow on and progress can be made

Mazarr et al. 22 [Michael J Mazarr, Michael J. Mazarr is a senior political scientist at the RAND Corporation. Previously he worked at the U.S. National War College, where he was professor and associate dean of academics; as president of the Henry L. Stimson Center; senior fellow at the Center for Strategic and International Studies; senior defense aide on Capitol Hill; and as a special assistant to the Chairman of the Joint Chiefs of Staff. His primary interests are U.S. defense policy and force structure, disinformation and information manipulation, East Asian security, nuclear weapons and deterrence, and judgment and decisionmaking under uncertainty. Mazarr holds a Ph.D. in public policy from the University of Maryland.; Brian Frederick, Bryan Frederick (he/him) is the associate director of the Strategy and Doctrine Program within RAND Project AIR FORCE, and a senior political scientist at the RAND Corporation. His research interests include strategic competition, interstate deterrence and escalation, conflict forecasting, military interventions, territorial disputes, international norms, the law of armed conflict, and regional security issues in Europe, East Asia, South Asia, and the Middle East. He has previously worked at the International Crisis Group, and the Issue Correlates of War Project. He completed his Ph.D. in International Relations at the Johns Hopkins School of Advanced International Studies (SAIS) in 2012, his M.A. from Johns Hopkins SAIS in 2002, and his B.A. in Philosophy from Williams College in 1998.; Emily Ellinger, Emily Ellinger is a policy analyst at RAND Corporation, based in the Pittsburgh office. Her research interests include strategic competition, alliance formation and politics, the security clearance process, extreamism, and security cooperation, geographically focused on Europe and East Asia. Ellinger holds a M.S. in international relations from the University of Edinburgh, Scotland. Her master’s thesis comprised a comparative analysis of US alliances as they related to intelligence sharing in a post-9/11 world. Her B.A. from Northwestern University is in Physics with concentrations in theoretical physics and astrophysics. During her undergraduate studies she spent three years researching protoplanetary disks with NASA, culminating in two publications including “Connection historical disk interactions with current planetary system architectures”. Prior to joining RAND, Ellinger was a threat analyst at Prescient LLC, a private firm that provided open-source analysis for on-the-ground threats and potential risks in remote locations around the world. During her undergraduate career, Ellinger spent a quarter in China studying at Peking University and Hangzhou Wanxiang Polytechnic. There she investigated public health and renewable energy technology and policy in a fellowship for the Wanxiang Corporation., Benjamin Boudreaux, Ben Boudreaux (*he/him*) is a professor at the Pardee RAND Graduate School and a policy researcher at RAND working in the intersection of ethics, emerging technology, and human security. His current research focuses on the ethics of artificial intelligence (including on algorithmic equity, biometric surveillance, and military AI) and on social media policy issues (such as misinformation). He leads the Pardee RAND Graduate School's ethics program, and teaches Ethics in Theory, Policy, and Practice and a course on complex systems policy design. Prior to joining RAND, Boudreaux was a diplomat in the State Department's Cyber Policy office, where he worked to promote security, stability, and human rights in cyberspace, and led State's cyber operations portfolio. He also has research interests in conflict prevention, Middle Eastern and South Asian regional issues, and international migration. Boudreaux holds a Ph.D. in philosophy from the University of California, Berkeley where he focused on ethical theory and political philosophy, a M.S. in foreign service from Georgetown University, and a B.A. in economics and philosophy from NYU. "Competition and Restraint in Cyberspace," RAND Corporation, https://www.rand.org/pubs/research\_reports/RRA1180-1.html] Blitz

Our analysis of the interests and perspectives of the major cyber actors, the character of norms and the cycle of norm emergence, and the history of cyber norm development highlighted two leading principles of a U.S. cyber norm strategy. First, it should be catalytic , seeking to encourage the gradual, sometimes messy process of political and social norm emergence rather than trying to put into place a singular treaty or agreement. Second, it should be multistakeholder, working with many public and private actors simultaneously to advance normative consen - sus on a broad front, and lending support to norm entrepreneurs. As discussed in Chapter Three, these principles—and many of the specific elements of this strategic approach described below— have characterized elements of U.S. policy on cyber stability and cyber norms since about 2011. Our argument is not that this general approach is entirely new, but that the emphasis in U.S. efforts should shift away from international expert negotiation and toward broader political engagement, as well as toward defining a small handful of normative limits with U.S. competitors and ensuring greater harmony between U.S. norm-promotion efforts and other U.S. activities in cyberspace.

### 2NC --- Perm do Both

#### Only a unilateral international actor solves – norms cannot be made through centralized authorities such as NATO

Raymond 20 [Dr. Mark Raymond, Dr. Mark Raymond is the director of the Cyber Governance and Policy Center at the University of Oklahoma. "Confronting the Ubiquity of Norms in Cyberspace and Cyber Governance," Lawfare, https://www.lawfareblog.com/confronting-ubiquity-norms-cyberspace-and-cyber-governance] Blitz

The Cyberspace Solarium Commission was tasked with applying social science insights to American cybersecurity strategy. Organization of the commission into three task forces on deterrence, active disruption of adversary attacks through persistent engagement, and norms-based regimes reflects an important truth. Norms, or [standards of socially appropriate behavior](https://www.jstor.org/stable/2601361?seq=1#metadata_info_tab_contents), are a ubiquitous and unavoidable dimension of global cyber policy. Distinguishing a norms-based approach, however, carries the risk of suggesting that a deterrence or persistent engagement strategy could be undertaken without relying on norms. In fact, norms are essential to both strategies and to any other possible cyber strategy. The only choices facing the United States (or any other actor) are about the *content* of the norms it promotes, and about how it will convince others to adopt, interpret, comply with and uphold them. Below, I introduce several vital but sometimes misunderstood features of how norms work and discuss their implications for American cybersecurity strategy. In the past 30 years, international relations scholars have learned a great deal about norms. First, norms often generate high rates of compliance without centralized enforcement; [internet technical standards](https://mitpress.mit.edu/books/protocol-politics) are a key example. Second, it is a [mistake](https://academic.oup.com/isq/article-abstract/59/2/238/1788767) for analysts to treat something that violates their own set of norms as something that is necessarily anti-normative. Individuals and groups across space and time have held vastly different notions about what constitutes appropriate behavior. Care should be taken not to conflate norms in general with a specific set of Western liberal norms that underpin contemporary rule-based global order. Third, norms are [not inherently likely to encourage cooperation or discourage violence](https://journals.sagepub.com/doi/abs/10.1177/1354066197003003003). Some norms (like U.N. Charter Article 51) explicitly authorize violence, at least under certain conditions. Thus, it is completely consistent with the standard definition of norms to envision an extremely conflictual world in which regular, high-consequence cyberattacks are regarded as appropriate behavior for major powers, states in general or even various nonstate actors. While such a world would not align with American interests or values, to the extent actors saw it as legitimate, it would reflect the influence of norms. Fourth, norms are not outcomes that remain static until they suddenly change. Rather, they are [ongoing products of social relations](https://www.cambridge.org/core/journals/american-journal-of-international-law/article/constructing-norms-for-global-cybersecurity/373A149D995A12E824E2FD1E0B5E5675) that exist not as individual things in isolation but as parts of complex normative systems that can (and often do) place actors in difficult positions requiring them to make determinations about appropriate behavior in light of multiple applicable norms that may be in conflict. Fifth, **this means that consensus and completeness** [**are not useful standards**](https://journals.sagepub.com/doi/10.1177/1354066107087766) **for thinking about** whether **norms** exist or can be useful in a given issue area. Finally, norms are important even when compliance is imperfect. They have a crucial role to play in responding to violations. The process of [applying and constantly adapting norms](https://global.oup.com/academic/product/social-practices-of-rule-making-in-world-politics-9780190913113?cc=us&lang=en&) highlights the fact that the international community relies on norms to provide a basis for criticizing or justifying behavior. It is the very existence of such behavioral standards that makes it possible to [stigmatize](https://www.cambridge.org/core/journals/international-organization/article/stigma-management-in-international-relations-transgressive-identities-norms-and-order-in-international-society/385D52A5CAC7C515491ED487781E3B4A) actions that fall outside expectations as with, for example, “rogue states.” In this way, norms are essential in justifying responses to norm-violating behavior, whether in the form of criminal indictments, economic sanctions or even the use of force. Other related norms tell us how to determine whether a prior norm has been broken, and how to respond if it has been What does this all mean for American cyber policy? A great deal. No single actor, however powerful, can unilaterally shape norms for cybersecurity. Doing so requires skillful, consistent engagement in global processes of rule-making, interpretation and application. Shaping cyber norms thus requires “persistent engagement” but of a very different kind than envisioned by most uses of the term. Specifically, norms development requires a coordinated whole-of-government approach led by the State Department. The United States must articulate and justify its positions in convincing, legitimate ways to a broad audience that includes industrial democracies, emerging economies, foreign and domestic firms, and civil society organizations. Since these stakeholders have [different standards](https://www.cambridge.org/core/journals/international-theory/article/multistakeholderism-anatomy-of-an-inchoate-global-institution/B69E6361B5965C98CFD400F75AA8DC53) for what makes an argument convincing, this presents an extremely challenging diplomatic task.

### 2NC --- Solvency

#### Disambiguating norms solves – it allows for accountability while avoiding the pitfalls of international agreements

Lewis 22 [James Andrew Lewis, Senior Vice President and Director, Strategic Technologies Program at CSIS, "Creating Accountability for Global Cyber Norms," Center for Strategic and International Studies, https://www.csis.org/analysis/creating-accountability-global-cyber-norms] Blitz

The year 2021 saw all UN member states agree in the Open-Ended Working Group (OEWG) on a [framework](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf) for responsible state behavior in cyberspace, based on norms developed in the United Nations Group of Governmental Experts (GGE) in 2015.1 The OEWG formalized global agreement on the 2015 norms. This consensus agreement means that the framework for responsible state behavior is now politically binding for all member states. Global agreement on the obligations for responsible state behavior is a substantial step forward in building international cybersecurity in a rules-based environment. Unfortunately, international experience since 2015 has shown that agreement on norms, even when politically binding, is by itself not enough to ensure their observation or create stability in cyberspace. This has shifted discussion from what norms are needed to how to build accountability and what to do when norms are ignored. While the norms agreed to by all member states will ultimately reinforce international stability, to make progress, it will be necessary to develop a collective diplomatic strategy to improve the observation of norms and increase accountability when they are ignored. A strategy of sustained engagement and the imposition of consequences is necessary for norms to have effect. Our assumption is that accountability for malicious cyber actions can only be strengthened if there are consequences for a state’s decision not to observe norms. If nothing else, a failure to take action in response to transgressions seems to only encourage opponents. An immediate task is to define the conditions for collective action. There has been an initial and informal agreement among like-minded democratic nations that accountability requires the imposition of consequences for a failure to observe norms, but several issues must be addressed. These include agreement on standards for attribution of the source of a malicious action and agreement on a proportional, lawful, and effective response. A collective approach is essential if efforts to create accountability are to succeed, and any response to a cyber incident will require political heft and sustained engagement. **Applicable Norms and “Agency”** What norms are in fact ignored? Many of the OEWG norms focus on protecting critical infrastructure. However, cyberattacks on critical infrastructure are rare. In contrast, risks of international peace and stability from other kinds of cyber actions are already increasing. If the aim is to increase stability, the relevant norms are found in [paragraphs 13(a) and (c)](https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf), where states agree to prevent actions that threaten or are harmful to international peace and security and to not knowingly allow their territory to be used for wrongful acts. This latter norm is vital, as it makes clear that responsibility derives from sovereign jurisdiction (or a failure to exercise it). This makes the assignment of political responsibility to a state easier and clearer. Equally important, the foundation for the OEWG norms is the binding agreement by all states to observe the UN Charter, where states have agreed to refrain from the use of force or threats to use force against the political independence of other states and have agreed to respect international law and fundamental human rights. These OEWG commitments and charter obligations are routinely ignored by some states that violate other nations’ sovereignty in ways that damage security, stability, and human rights. One shortcoming with the UN-agreed norms is their lack of “agency,” or the capacity to take action. In theory, agency falls to the international community acting through the United Nations Security Council (UNSC), but in fact, this means the ability to reach agreement in the United Nations on a response to malicious cyber action is very limited. The United Nations is a consensus-based organization, with many members who have different and sometimes competing interests. Creating accountability has always been difficult for the international community, not just in cyberspace. Actions must be exceptionally egregious, and powerful states will put their national interests first. Additionally, states are understandably reluctant to agree to coercive measures—particularly those involving force or the threat of force—for cyber incidents where culpability is deniable, rules are still unclear, and damage (from a strategic perspective) is usually minimal. The absence of consequences for individual cyber actions makes it easy to ignore efforts to impose accountability. *One shortcoming with the UN-agreed norms is their lack of “agency,” or the capacity to take action. In theory, agency falls to the international community acting through the United Nations Security Council (UNSC), but in fact, this means the ability to reach agreement in the United Nations on a response to malicious cyber action is very limited.* Creating accountability is complicated for cyber actions, since almost all such actions stay below the threshold of the use of force, on which many rules are predicated. The international community is more likely to respond to the use of force, but few cyber incidents have had effects that approximate the use of force. Despite hyperbole, no one has ever died in a cyberattack, there have been very few incidents of physical destruction, and until 2020, cybersecurity had never come before the UNSC, making it a lesser issue in the eyes of many member states not directly involved in cyber conflict. This is changing as the risks of malicious cyber action have increased, as dependence on networks has grown, and as a result of increased great power competition. Even so, there is still some reluctance to act in response to malicious cyber action. Diplomatic practice does offer an alternative approach that provides for agency. This alternative is more attainable in the near term. It requires a group of like-minded nations to first agree on their responsibility to observe cyber norms in their national practice. This requires a public commitment at senior political levels for these nations themselves to be guided by the OEWG framework for responsible state behavior. On the basis of this commitment, the second step is collectively responding to violations of norms. This collective response has rarely been undertaken for malicious cyber actions. Changing this is a crucial first step. Consistent action by a group of states to impose consequences for not observing agreed norms is essential to creating accountability. An example might be the Western effort in the 1990s to persuade China not to sell missiles.2 This effort took several years of high-level engagement and a constant reiteration of the need for responsible states to observe the norms developed for such transfers (in the Missile Technology Control Regime). The issue was raised with China at every level, on every occasion, and during every topic of engagement. A talking point on proliferation was appended to every senior officials’ statement. Most importantly, it was not just one nation appearing to complain and suggest; it was done repeatedly and collectively every time Western leaders engaged with their Chinese counterparts. One of the most important steps that can be taken to increase observation of the 2021 UN norms is to make this kind of sustained engagement a routine expectation for state behavior rather than a sporadic objection when unspoken expectations for respecting sovereignty and law are flouted. Raising specific instances of a failure to observe norms with the state responsible and asking for explanation and cessation is an essential first step. However, such efforts will be more effective when accompanied by persuasive evidence (and adequacy will be discussed later) and when carried out by many nations. This can be done in both private and public engagement. In the proliferation case, it was persuasive to share with China and others the most senior levels of intelligence (such as satellite imagery) that established responsibility. For cyber actions, there will be objections to such sharing on the grounds that this will inform opponents of U.S. capabilities, but the detailed indictments made by the Department of Justice—often accompanied by pictures of the individual government agent—show such sharing can be done. This is different from “name-and-shame,” a useless strategy involving a public statement made safely in capital and without any follow-up action. These statements have no political weight. What is needed is a direct engagement with the leaders of culpable states and the credible threat of a punitive response. The key to a new approach is a consistent, collective, and direct approach at senior levels to object to a state’s failure to observe norms accepted by all responsible states. Every time ministers meet with a counterpart, they must raise the issue of malicious cyber action, using points developed in common with their partners and providing specifics of the act. The actions that have come closest to this have only occurred with the joint condemnations of [China](https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/) and [Russia](https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise) and the statements [by President Biden](https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/16/remarks-by-president-biden-in-press-conference-4/) and the EU high representative for foreign affairs and security policy, [Josep Borrel](https://www.euronews.com/2021/09/24/eu-s-borrell-threatens-sanctions-on-russia-over-malicious-cyber-activities). But if such statements are to be more than one-offs, filed away and ignored, they must be repeated by all other G7 nations and by other EU member states. Consistent and direct iteration on the need to observe norms must become standard diplomatic practice for like-minded states. A comprehensive strategy to create accountability would define and articulate possible responses to reinforce an integrated diplomatic campaign. In developing a collective diplomatic strategy linked to potential consequences, the issues of political attribution, the development of a menu of response actions consistent with international law and agreed norms, and proportionality in any response come to the fore as determinative issues.

### 2NC --- Coop Fails

#### International cyber agreements always fail – history proves

MaČÁK 17[Kubo MaČÁK, Dr Kubo Mačák is a legal adviser at the International Committee of the Red Cross (ICRC). Prior to joining the ICRC in 2019, he worked as an Associate Professor of Public International Law at the University of Exeter in the United Kingdom. "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers," Cambridge University press, https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5] Blitz

2. Crisis indicators: International law and cyber security Three stand-out indicators suggest a crisis in this area of law. First, the domain of cyber security appears resistant to codification of the applicable rules in a comprehensive multilateral binding treaty. [25](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn25) This is not for want of trying by the leading international stakeholders. In 1996, France put forward the earliest proposal with the lofty title *Charter for International Cooperation on the Internet*. [26](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn26) Later, a Sino-Russian initiative resulted in two proposals for a *Code of Conduct for Information Security*, submitted to the UN General Assembly in 2011 and 2015, respectively. [27](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn27) However, none of these proposals was met with much enthusiasm by other states [28](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn28) and scholars describe the prospects of an ‘omnibus’ treaty being adopted in the near future as slim to negligible. [29](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn29) This is no doubt partly because, whatever the subject, the ‘very word “treaty” may conjure up the fearsome formalities of diplomacy’, with a chilling effect on states’ willingness to engage in this form of law-making. [30](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn30) Yet, with respect to cyber security, this aversion appears to be particularly pronounced. Second, states have shown extreme reluctance to contribute to the development of cyber-specific customary international rules. In addition to state practice in this area being inevitably shrouded in secrecy, [31](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn31) states have been reluctant to offer clear expressions of *opinio juris* on matters related to cyber security. [32](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn32) At times, this approach may be understandable, as it is the consequence of domestic political gridlock or a deliberate waiting strategy. [33](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn33) On other occasions, it may rather be due to the persistent ‘cybersecurity knowledge gap’; in other words, the striking lack of understanding of cybersecurity permeating governments around the world. [34](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn34) On the whole, this reluctance adds to the pervasive ambiguity as far as the specific applicability of international law is concerned. This trend is visible even in the most recent developments. A representative example of another missed opportunity to steer the development of cyber custom is provided by the recent US *Law of War Manual* adopted in July 2015 and updated in December 2016. [35](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn35) Although it does contain a chapter on cyber operations, [36](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn36) the *Manual* skirts virtually all unsettled issues, including standards of attribution, rules of targeting or the requirement to review cyber weapons. [37](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn37)

## Open source

### 1NC --- Open Source

#### The United States Federal Government should

#### renew its commitments to 18F and the Federal Source Code Policy

#### require [Insert Object of Plan] to meet ISA/IEC 62443 series of standards

#### open source its code for [Insert Object of Plan]

#### Federal open-sourced policy gets modeled globally

Tucker 22 - [Margaret Tucker, (Platform Policy Analyst for GitHub), 6-14-2022, "How can the United States build its Open Source Software policy?," GitHub Blog, <https://github.blog/2022-06-14-how-can-the-united-states-build-its-open-source-software-policy/> ]//MLee

The world runs on open source, which serves as the foundation for globally interconnected digital infrastructure. With an estimated [97% of codebases containing open source](https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2022.pdf), both the private and public sectors depend on the maintenance of open source software (OSS), but governments have untapped potential as leaders in the OSS community. Currently, most engagement has centered around security. Earlier this year, GitHub attended the [White House meeting on software security](https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/) where participants discussed the unique value and security challenges of OSS. While securing OSS is an important concern, full stack federal OSS policy requires dialogue between policymakers, practitioners, and wonks. To this end, GitHub was proud to attend the June 8 roundtable discussion, [From Procurement to Policy: Towards OSS Infrastructure](https://www.eventbrite.com/e/from-procurement-to-policy-towards-oss-infrastructure-tickets-318956335987), in Washington, D.C.

The event kicked off with a bold question posed by Harvard Business School professor, Frank Nagle: “What would a federal open source policy agenda look like?” Building off of his [Brookings policy brief](https://www.brookings.edu/research/strengthening-digital-infrastructure-a-policy-agenda-for-free-and-open-source-software/), Nagle proposed actionable steps the public sector could take to cultivate a thriving OSS ecosystem, from understanding and supporting the open source ecosystem to establishing a federal Open Source Program Office (OSPO). A federal OSPO could coordinate OSS efforts across agencies, including those among the thousands of government organizations around the world already using [GitHub for government work.](https://government.github.com/community/) As the meeting progressed, speakers addressed the political and organizational challenges to federal open source publishing and discussed how renewed commitment to [18F](https://github.com/18F/open-source-policy/blob/master/policy.md) and the [Federal Source Code Policy](https://www.cio.gov/2016/08/11/peoples-code.html) could bolster US support for digital infrastructure.

Digital infrastructure is global, and US OSS policy should reflect the globally interconnected nature of OSS contributors while building domestic capacity. To that end, [OpenForum Europe](https://openforumeurope.org/) presented a survey of EU open source policy objectives and [how governmental OSPOs can learn from the private sector](https://openforumeurope.org/what-can-governmental-ospos-learn-from-the-private-sector-ones/). Explaining the architecture of Germany’s [Sovereign Tech Fund](https://sovereigntechfund.de/en), speakers argued that OSS policy is about more than simply public sector adoption, but also using strategic funding and legal mechanisms to support healthy and secure OSS. When it comes to OSS support, sustained funding is crucial. When support for the Open Technology Fund was at risk, [GitHub joined the public call to renew support](https://github.blog/2020-07-02-github-supports-the-open-technology-fund/). Finally, the Digital Impact Alliance presented the [Digital Public Goods Charter](https://dial.global/charter/), a multistakeholder effort to enable developing countries to build safe, trusted, and inclusive digital public infrastructure at scale. GitHub affirms that OSS is a public good, and has launched research projects to [define a list of platform usage metrics by country for international development, public policy, and economics disciplines](https://github.blog/2021-08-31-request-for-proposals-defining-standardized-github-metrics/), as well as [measure the economic impact of open source](https://github.blog/2022-01-20-open-source-creates-value-but-how-do-you-measure-it/).

### 2NC --- Solves Cybersecurity

#### Open-sourced software solves cybersecurity

Lin 22 - [Sz Lin, (works for Moxa in the Software Development Center) 2022, "Manage Vulnerabilities in ICS Open Source Software," Global Cybersecurity Alliance, <https://gca.isa.org/blog/manage-vulnerabilities-in-ics-open-source-software>] //MLee

Open source software (OSS) is frequently integrated into industrial control systems (ICS) and critical infrastructure as business owners pursue greater interoperability, portability, and interchangeability. While tapping into the benefits of open source software, cybersecurity considerations are imperative, since availability and reliability is paramount for industrial control systems. Ensuring high-quality code in open source software to avoid an increased cyber risk to the ICS becomes a pivotal challenge. Vulnerability management of open source software should be considered and evaluated through the lifecycle of software development, starting as early as possible—to reduce cost and effort in the maintenance phase and to enhance the cybersecurity management that helps avoid system downtime.

Open Source Software in Industrial Control Systems

OSS is ubiquitous nowadays. According to a report by Synopsys Cybersecurity Research Center, OSS is widely adopted across various industries, including the Internet of Things (IoT), cybersecurity, and internet and mobile apps.1 Microsoft, once the largest proprietary software advocate, is now the single largest contributor to open source projects in the world.2 With tech giants such as Facebook, Google, Amazon, and Apple all involved in various open source projects nowadays—contributing to, as well as consuming, millions of lines of open source code daily—the prevalence of open source is evident in today’s technology development.

Besides consumer-grade hardware and software, OSS also proliferates in industrial control systems and critical infrastructure. Linux, the open source operating system (OS) based on Linux kernel, is now a mainstream OS in the industrial space.

For instance, take operational technology (OT) systems. From industrial PCs and programmable logic controllers (PLCs) in the control network at the field level, to the supervisory control and data acquisition (SCADA) and engineering servers in the supervisory network at the mid-level, to application servers in the management network at the top level, a majority of these industrial control devices run Linux OS with open source applications.

OSS provides great interoperability, portability, and interchangeability to ICS, as numerous devices may all come from different vendors in the supply chain with heterogeneous software packages. The “open” nature of OSS allows ICS providers and industrial device suppliers to integrate systems with ease and flexibility while effectively enhancing the efficiency of software development without building things up from scratch.

The Cybersecurity Requirement for ICS

However, the “open” nature of OSS also raises cybersecurity concerns in ICS. After all, the vulnerabilities or cybersecurity issues in the ICS and critical infrastructure may result in far-reaching impacts such as a massive power outage and/or operations failures in the civil infrastructure systems across telecoms, the water supply, wastewater treatment, and railways, to a certain extent. To tackle the cybersecurity threat to ICS, worldwide governments,3 including the National Institute of Standards and Technology (NIST) under the U.S. Federal Government, have strongly recommended that ICS owners comply with certain standards for industrial cybersecurity, such as the ISA/IEC 62443 series of standards.

ISA/IEC 62443-4-1, one of the ISA/IEC 62443 standards, defines a secure development lifecycle for the purpose of developing and maintaining secure products used in industrial automation and control systems. To meet the requirement of security, reliability, and sustainability for an ICS, it is critical to manage the great amount of OSS running in the ICS during the software development lifecycle (SDLC), as part of the product life cycle specified by the ISA/IEC 62443-4-1 standard.

## Space

### 1NC --- SpaceX

#### SpaceX bottom up approach solves – bringing the public and private sectors together solves without relying on international actors.

Brian Downey, 9-2-2020, "MSP Security Threats," Connect Wise, <https://www.connectwise.com/blog/cybersecurity/improving-msp-cybersecurity-a-look-at-spacex>

If you’ve been following the news lately, you know that SpaceX—the space exploration company founded by Elon Musk nearly 20 years ago—is making a lot of headway in their mission to get to Mars. It’s not a matter of IF SpaceX will make human travel into space possible, but WHEN.

There’s a lot to be learned from the way SpaceX approaches their mission, specifically as it relates to cybersecurity.

It may seem like a stretch to link something like space travel to cybersecurity, but a strong connection can be made based on the way SpaceX runs its business.

Let’s explore how managed service providers (MSPs) can learn from SpaceX.

Bottoms up approach to solving issues

Oftentimes, companies who are venturing into new territory have a tendancy to choose to take what they have and improve it versus stepping back and understanding the problem and being open to starting from scratch. When you think about SpaceX, they could have taken rocket ship components from the 1950s and 60s and thought about what needed to be added to it as had been the approach for the past 50 years. Instead, SpaceX took a ground-up approach and started fresh.

As a result of that ground-up approach, SpaceX streamlined the way they solved problems. A very good example of this is when you look at the views from the inside of the SpaceX Dragon cabin. The difference is obvious when you look at the variety of gauges and screens in the legacy NASA shuttle versus the four clean looking screens in the Dragon cockpit. The SpaceX team focused on what information was needed, leveraged various pieces of data traditionally shown independently, and understood how they could display that data within their consoles to deliver useful messages to astronauts. This changed the way astronauts solved problems. Where in the past, astronauts needed to take multiple pieces of independent data and execute calculations to answer their questions, today, those components work with and talk to each other to give operators the exact information they need in a more holistic way.

In other words, in old shuttles, every single piece of information possible was given to an operator. In SpaceX, only the information that is needed right now is provided.

As an MSP putting this in a cybersecurity lens, it can be very tempting to approach new security problems by taking your existing infrastructure, understanding any gaps, and bolting a few more tools on to try to close them. This approach leaves you with a management approach akin to trying to make sense of all the data points in the legacy shuttle. Instead, you should look at the problems you need to solve and identify the full tech stack and offerings to meet the needs of people today. The goal with cybersecurity is to understand and predict what happens when certain actions are orchestrated together.

Teams joining together

The way that SpaceX has brought the public and private sectors together is a groundbreaking facet that cannot be ignored. For the most part, private companies work independently and the public sector operates in a completely different world. SpaceX is bridging the two together by functioning as a private company working alongside public sector employees.

When you think about MSPs and their clients, much of the work they do is in isolation of one another. A law firm, for example, looks at an MSP as having responsibility for all things technological, while an MSP has no interest in doing what the law firm does. With cybersecurity, this needs to change. MSPs and clients need to see security as a joint approach.

Going back to the law firm, an MSP can do everything on their end to protect their client, but if an employee in that law firm is going to bad websites and using weak passwords, they can create cybersecurity risks that an MSP can’t counteract. It’s not just about an MSP educating their client, but also about the client feeling empowered and believing that cybersecurity is important, not an inconvenience.

If NASA didn’t truly believe that Elon Musk and his team could successfully enter the space industry, they would have never worked with SpaceX to solve hard problems along the way. The mutual belief about the importance of SpaceX’s work was greater than the perceived inconveniences to get there, therefore resulting in a successful joint partnership.

Working towards a bigger mission

The mission to get to Mars is a pretty overwhelming, boil-the-ocean type of task, right? That’s how a lot of people feel about cybersecurity.

The key is to break everything down into smaller pieces that will eventually help you reach your larger goal. SpaceX isn’t just building a rocket and attempting to get to Mars on the first try. They are running small tests little by little that will help drive them towards overall success. Their most recent flight didn’t actually go somewhere or do an activity that hadn’t been done before. But it proved that they could do what has been done before with new equipment, a new approach, and a new team that appears to be capable of their larger goal, and that makes us all feel confident that they will get to that larger goal.

Smaller, more attainable goals are key for any MSP getting into cybersecurity. Focus on the first step and then the second step and so on versus zoning in on how far you are from your end destination.

Additionally, with SpaceX and with cybersecurity, this story is larger than any of us. There’s a social advantage to playing a role here.

SpaceX is trying to help the human race survive after Earth is no longer here. With cybersecurity, MSPs are protecting the people and institutions within our countries and society.

Everyone wants to leave a legacy, and contributing to something that will potentially make our society a better place is a significant way to do so. MSPs need to realize they aren’t just identifying and stopping faceless threats, they are working to stop efforts to destabilize our society, to impact political processes and subvert global crime organizations that are involved in much more than ransomware or selling data. The work MSPs do to protect their clients is truly substantial at a global level.

In conclusion

SpaceX appears to be the future of space travel and will disrupt the way we think about and approach space exploration in the future, the same way cybersecurity is the future for MSPs. It’s the next frontier. While it may be challenging and overwhelming to think about, it’s enormously beneficial and kind of a necessity for us to think about right now.

Anytime there is a revolutionary shift, it creates an opportunity for businesses to decide how to work. SpaceX is changing everything about the way we think about space travel. Cybersecurity is disrupting and changing everything about the way we deliver services to IT clients. MSPs need to embrace that disruption and capitalize on it.

### 1NC --- Space Force

#### The USSF solves satellite cyber security

Johnson 22 - [Kimberly Johnson, (Writer covering aviation and defense issues, including assignments in Iraq and Afghanistan with Marine Corps and Army infantry units) 5-26-2022, "To Infinity and Beyond," FLYING, [https://www.flyingmag.com/to-infinity-and-beyond/]//MLee](https://www.flyingmag.com/to-infinity-and-beyond/%5d//MLee)

The U.S. Space Force (USSF)—the nation’s newest military service branch and the first created in a generation—stands ready to engage in a new era of national defense where commercial space and military interests collide.

Pushing military capabilities “to infinity and be-yond” isn’t exactly new. The U.S. military began space research following World War II and prior to the formation of the Department of the Air Force. Nearly four decades later, the U.S. Air Force (USAF) unified efforts by establishing the Air Force Space Command in 1982. That mission later expanded into cyberspace as well as providing space-based communication and navigational support for U.S. forces deployed in Iraq and Afghanistan.

In December 2019, the command was authorized to stand alone when Congress gave the green light to the creation of the new service through the National Defense Authorization Act. When it was signed into law, it marked the reality that space creates a new frontier when it comes to national security. The need for a new service focused on defense in space comes as adversaries, such as China, increasingly modernize their military capabilities. U.S. military leadership keeps a wary eye on China’s growing inventory of hypersonic weapons, anti-satellite systems and cyber and electronic warfare capabilities. “While America is still the dominant military power on the planet today, we are being more effectively challenged militarily than at any—any—other time in our history,” Secretary of the Air Force Frank Kendall said at the Air Space Cyber Conference in September 2021.

That challenge is no longer strictly terrestrial. In an era of commercial space tourism and satellite dependence, space has gone from a benign environment to a contested one, according to one top Space Force official.

“We don’t have decades. We’re in a race with some serious adversaries that mean to deny us those advantages that we get in space,” says Lt. General B. Chance Saltzman, USSF deputy chief of space operations. Russia and China are pursuing and using kinetic and non-kinetic space weapons, “some operating on the ground, pointing up. And some that are designed to work from orbit,” Saltzman says. Some of those systems include directed energy, jammers, and satellite kill vehicles, he says.

In addition, there are currently nearly 30,000 tracked space debris objects in orbit, prompting the monitoring of more than 1,500 that have the potential for collision at any given time, he adds. “Space has truly become a congested and contested environment,” Saltzman says.

Built for Speed

The Department of the Air Force’s Space Force, which currently has nearly 7,000 uniform-wearing guardians, is a coequal branch of service alongside the USAF. It consists of a simplified structure of three field com-mands: Space Operations Command (SpOC), Space Systems Command (SSC) and Space Training and Readiness Command (STARCOM).

With a streamlined headcount of personnel expected to grow to 8,400 in the coming fiscal year, standing up the new service has been an exercise in building some-thing new while also culling layers of bureaucracy, says General John W. “Jay” Raymond, USSF chief of space operations. “We wanted to have a purpose-built organization, built for speed. Something that could go fast. Something where we can push decision making down to the lowest level, and something that we could get layers of bureaucracy out of the way,” Raymond says.

The USSF’s focus on speed means senior leadership infield commands will have more authority and resource sat their disposal. “SSC needs to re-energize its approach to seeing, understanding, and rapidly developing while fielding new capabilities to keep us ahead of threats that we see from China and others,” says USSF Vice Chief of Space Operations General David D. Thompson.

Picking up the pace means that the Space Force will also need to expand partnerships when it comes to acquisitions, Thompson says. “Commercial companies are moving so rapidly. We need to develop partnerships with the commercial sector to understand what they are doing as well as be able to leverage it to our benefit.”

### 2NC --- Satellites

#### Updating satellites solves critical infrastructure.

Rebecca Heilweil, 7-29-2021, "For hackers, space is the final frontier," Vox, <https://www.vox.com/recode/22598437/spacex-hackers-cyberattack-space-force>

Our increased reliance on this tech makes the threat of hacking especially worrisome. A hacker could try to access a satellite by targeting a company’s ground systems, and once inside, the attacker could manipulate the communications or controls, download unwanted software, or even tell the satellite to change its course, according to Iain Boyd, the director of the University of Colorado Boulder’s Center for National Security Initiatives.

“It’s the same kind of thing where people are getting into your computer system and behaving badly,” Boyd told Recode. He added that hackers might also attempt to overwhelm a satellite with false signals or impersonate a satellite’s communication — a process called spoofing — to confuse vehicles on Earth’s surface.

These cyberattacks on space systems have been disruptive, but their impact could be catastrophic. For instance, in 2014, US officials blamed China for a cyberattack that forced the National Oceanic and Atmospheric Administration (NOAA) to cut off public access to imagery data from a satellite network used for weather forecasting. Russia has reportedly used GPS spoofing to confuse ships about their actual locations. And in the future, a worst-case scenario could involve a hacker tricking a satellite into crashing into other space infrastructure, according to William Akoto, an international politics professor at Fordham University, who studies cyber conflict.

“You can’t just walk down to the server room and apply a patch to something that’s in orbit,” explained Matthew Scholl, who leads the computer security division of the Information Technology Laboratory at the National Institute for Standards and Technology (NIST).

To address the impending threat of cyberattacks on space systems, the US military earlier this year transferred more than 2,000 cybersecurity experts to the newly formed Space Force. The Air Force, meanwhile, has begun hosting competitions encouraging hackers to break into satellites, with the hope of learning more about potential vulnerabilities. But cybersecurity experts warn that the private space industry hasn’t been transparent about how it’s managing security threats.

“From a commercial standpoint, we have to hope that they’re doing something,” said Falco, the Johns Hopkins professor. “But most commercial companies working on satellite systems have given zero details about anything that they have regarding the security of their space systems.”

Some of these companies are currently hiring cybersecurity professionals. Blue Origin, for instance, has been looking for an information system security officer to find vulnerabilities in the company’s systems, while SpaceX is searching for an information security assurance analyst to investigate the physical and cybersecurity of the company’s supply chain.

None of the companies Recode contacted — Virgin Galactic, Blue Origin, OneWeb, and SpaceX — responded to a request for comment about the state of their cybersecurity.

But as commercial space companies try to staff up their security teams, the federal government is also stepping in to help.

Last year, then-President Donald Trump signed an executive order recommending principles for cybersecurity and space systems, encouraging private companies to take precautions like boosting protections for control systems in their rockets and satellites and deploying antivirus software to protect their ground stations. NIST has developed cybersecurity resources for commercial space operations, including satellites.

In June, Reps. Ted Lieu and Ken Calvert proposed legislation that would classify space as critical infrastructure to boost collaboration between private space companies and the government on cybersecurity matters. The Federal Aviation Administration also helped create the Space Information Sharing Analysis Center (Space ISAC), a collaboration that coordinates with companies across the space industry to share information about potential threats and attacks to their cybersecurity.

“Infrastructure that is distributed globally means that there’s a very broad attack surface,” Erin Miller, Space ISAC’s executive director, told Recode. “We need to be building in and designing cybersecurity capabilities into every single one of our space systems.”

For now, that means that ensuring national security and addressing the cybersecurity challenges of the emerging space industry are one and the same. After all, the growing number of attacks against all sorts of private companies, whether they’re oil pipelines or meat distributors, makes it clear that when firms don’t protect themselves from hackers, the American public can feel the consequences. As more of the tech that powers our everyday lives heads to space, so should the country’s increased focus on cybersecurity

## Ukraine

### 1NC --- Ukraine

#### The United States Federal Government should

#### declare that Ukraine will not be admitted into the North Atlantic Treaty Organization

#### remove its offensive nuclear missiles from Russia’s borders

#### US unilateral action solves Ukraine escalation

Freeman 22 - [Robert Freeman, (Founder and Executive Director of [The Global Uplift Project](https://tgup.org/) which builds small-scale infrastructure projects in the developing world to improve humanity’s capacity for self-development; author of "The Best One Hour History" series which includes "World War I" , "The InterWar Years", "The Vietnam War", and other titles.) 3-7-2022, "How the US Could Solve the Ukraine Crisis Tomorrow: If the U.S. wants peace, it can have it tomorrow." <https://www.commondreams.org/views/2022/03/07/how-us-could-solve-ukraine-crisis-tomorrow>] //MLee

No war is a one-sided affair. There is no sound to one hand clapping. Russia's assault on Ukraine is an unambiguously bad thing. But it didn't happen in a vacuum. In order to solve the problem, we have to first understand the context in which it occurred, and the part that the U.S. played in its happening. [The U.S.] can attain that end with two simple moves: declare that Ukraine will not be admitted into NATO; and remove its offensive nuclear missiles from Russia's borders. The Big Bang in U.S.-Russian relations was the breakup of the Soviet Union in 1991. Then-U.S. president George H.W. Bush and his Secretary of State, James Baker, promised Mikhail Gorbachev that if he agreed to the unification of Germany, NATO would not expand eastward, toward Russia, "not one inch." That promise was broken almost immediately when, in 1999, Bill Clinton helped usher Poland, Hungary, and the Czech Republic into NATO. Russia considered this move not just a betrayal, but an act of aggression. First, Poland is an implacable enemy of Russia, and has been for centuries. And NATO had just finished bombing Russian ally Yugoslavia out of existence. The "slav" in Yugoslavia signifies the same ethnicity as the Slavs who are the Russian people. It is lost on the average American that Russians are spooked by Western aggression. Napoleon invaded Russia in 1812 and burned Moscow to the ground. That's what Tchaikovsky's 1812 Overture, with its church bells ringing and cannons booming, is about. The German invasion in the First World War caused the government of the Tsar to fall to the Bolsheviks. That gave birth to communism as a state-based system and the animus for the Cold War which dominated the second half of the Twentieth Century. Before World War I was even settled, the Western victors invaded Russia to try to snuff out its new government before it was stable. That was the infamous White Counter-Revolution, led by the U.S., the U.K., Japan, and Italy. The German invasion in World War II caused the death of 27,000,000 Russians, 90 times U.S. losses in the War. Over 70,000 villages, 1,500 towns, and 9,000 bridges were destroyed. The already primitive national transportation network was reduced to rubble and agricultural production was decimated. Russians remember these things, though they are barely known in the West. The perception of aggressiveness in NATO moving eastward was hardly the Russians' alone. Bill Bradley, Paul Nitze, Sam Nunn, Robert McNamara, and more than 30 other foreign policy heavyweights wrote to Clinton that such expansion was both provocative and unnecessary, given the absence of a military threat. George Kennan, the pre-eminent U.S. strategist of the post-World War II era, declared that, "NATO expansion will prove the greatest U.S. foreign policy blunder of the twentieth century." That is a pretty stern prediction, coming from the man who conceived of the Cold War policy of Containment and who, in 1980, wrote, "The Vietnam War was the most disastrous of all of America's undertakings over the whole two hundred years of its history." It didn't matter. The U.S. had just won the Cold War. It was on a roll, convinced of its imperial inevitability, strategic infallibility, and military invulnerability. Vapid phrases masqueraded as deep ideas, phrases like "a new world order," "the end of history" and "the indispensable nation." They were tossed around as rationalizations for the use of force against any nation that stood in the way of U.S. pursuit of global hegemony. Think, Iraq, and Afghanistan. The U.S. promise to not move NATO eastward was broken again, in 2004, when, during the George W. Bush administration, NATO admitted Estonia, Latvia, and Lithuania to membership. All three nations adjoin Russia, placing NATO forces on Russia's borders. NATO also admitted Romania and Bulgaria in the same induction batch. Poland, Hungary, and Romania participate in NATO's "nuclear preparedness posture" which means hosting offensive nuclear missiles aimed at Russia. These can hit major Russian cities in as little as 10 minutes. The best way to understand the provocativeness of this move to the Russians is the Cuban Missile Crisis. In 1962, the Soviet Union began placing offensive nuclear missiles in Cuba, 90 miles off the coast of Florida. It was in response to the U.S. having installed similar missiles in Turkey. The Cuban missiles would be able to hit Washington D.C. in 30 minutes. The U.S. became apoplectic, in fact, hysterical. There was no defense against the missiles. U.S. military forces were put on "DEFCON 2" alert, the highest state of preparedness short of actual war. It was the only time during the entire 45 years of the Cold War they were placed at such an elevated state of readiness. Robert McNamara, then Secretary of Defense, later wrote of going out onto the balcony of the White House, looking up at the stars, and crying. It occurred to him that this would be the last Saturday he would ever see. That's how perilous the Crisis was. It was only John Kennedy's deft handling of the situation that defused the Crisis. Part of the resolution was that the U.S. agreed to remove its missiles from Turkey. It was an implicit acknowledgement on the part of the U.S. of just how provocative such forward-based offensive nuclear systems are. They are no less provocative today. In 2014, the U.S. helped carry out a coup d'état against the democratically-elected, Russian-leaning Ukrainian government of Viktor Yanukovych. It installed in its place a crypto-fascist, Western-leaning government headed by Arseniy Yatsenyuk. U.S. Assistant Secretary of State Victoria Nuland was recorded organizing the coup. The recordings were made public by Russian intelligence in February 2014. When told by her associate, Geoffrey Pyatt, that the EU would not support a coup, Nuland famously declared, "Fuck the EU." Since the 2014 coup, the U.S. has shipped more than $2.5 billion in weapons to the new Ukrainian government. It has seen to it that Ukraine has not honored the Minsk I and II treaties that it signed in 2014 and 2015. Those treaties were designed to protect the autonomy of Russian-speaking dissidents in eastern Ukraine. In early February, the government of Ukraine began shelling Donbass, that eastern region of the country with a majority Russian-ethnic population. This has been done with the implicit blessing of the U.S., Ukraine's strategic sponsor Between 2002 and 2020, the U.S. withdrew from the Anti-Ballistic Missile Treaty, the Intermediate Range Nuclear Forces Treaty, and the Open Skies Treaty. All were designed to reduce tensions with Russia by ensuring verifiable enforcement of strategic nuclear weapons systems. Without the Treaties, nuclear uncertainty, and, therefore, the risks of mis-step and war, are greatly heightened. So, where does this leave us? Harvard's Stephen Walt, hardly a lightweight or a leftist dove, wrote two weeks ago, "Whatever your views on NATO enlargement might be, there is overwhelming evidence that Russian leaders were alarmed by it from the start and expressed their concerns repeatedly. Moscow grew increasingly opposed …as NATO crept ever eastward." Nobody can pretend the West did not know what the stakes were or what was coming. No meaningful security guarantees were offered. Indeed, in December, 2021, Vladimir Putin stated publicly that there was no further back that Russia could go. If the west would not provide meaningful security guarantees, Russia would solve the problem itself through "military-technical measures." The current invasion is what he was referring to. Nobody can pretend the West did not know what the stakes were or what was coming. No meaningful security guarantees were offered. Again, Russia's invasion of Ukraine is unambiguously bad. But as we search for a solution to the crisis, the key consideration is that while Ukraine is existential for the Russians—a matter of life and death—it is not a vital national security interest to the U.S. This is revealed in President Biden's repeated assurances that no U.S. forces will be committed to Ukraine. That is the key to the solution. If the U.S. is sincerely interested in a peaceful resolution of the crisis—and for argument's sake, let's assume that it is—it can attain that end with two simple moves: declare that Ukraine will not be admitted into NATO; and remove its offensive nuclear missiles from Russia's borders. Since Ukraine is not a matter of strategic interest to the U.S., this would come at little cost to the U.S. but will yield vastly disproportional gains to the situation by facilitating immediate de-escalation. Both the U.S. and NATO have stated informally that Ukraine will not be admitted anyway, so nothing, save, perhaps a little face, is lost. It would allow Russia to withdraw with something to be said for its efforts. As for the second plank of the solution—withdrawal of U.S. nuclear missiles from countries adjoining Russia—the U.S. understands better than any nation on earth the value of having offensive nuclear missiles removed from its borders. It knows, from first-hand experience, better than any nation in the world, how to defuse this crisis. This is the concept of "strategic empathy:" understanding your adversary's interests and motivations, not to give in to them, but to better attain your own ends. As Walt, Kennan, and other analysts have said, Russia feels aggressed upon, threatened, and out of peaceful options. If the U.S.'s ends are peace, the means are at hand to achieve it, and with no loss of strategic position. If the U.S.'s interests are not peace, that will be revealed equally as clearly, equally as quickly. Yes, there will be necessary negotiations about withdrawal, reparations, and other such wind-downs, but those pale next to the threat of unintended escalation to what could very easily end up as nuclear war. The stakes are huge. Simple, workable solutions are at hand. The costs are small. The alternatives are unfathomable. If the U.S. wants peace, it can have it tomorrow.

# Biotech

## CBD

### 1NC --- CBD

#### Plan text: The United States Federal Government should ratify the Convention on Biological Diversity and take action to complete and sign the Biosafety Protocol

#### The CBD and BSP work to protect biodiversity and increase information sharing between countries for mutual benefit of the environment and the field of biotechnology

BIO (Biotechnology Innovation Organization, BIO is the world’s largest advocacy association representing member companies, state biotechnology groups, academic and research institutions, and related organizations across the United States and in 30+ countries, “The Biosafety Protocol-An Overview”, <https://archive.bio.org/articles/biosafety-protocol-overview>, Accessed June 19, 2022)//AS

“Representatives from 170 countries are currently negotiating international provisions governing the shipment and use of products from biotechnology. These provisions, officially known as the "Biosafety Protocol," are intended to provide uniform international requirements for ensuring the safe transport and use of these products. The Protocol could offer a framework to guide countries that currently lack national regulatory systems for products of biotechnology. If the Protocol is not carefully crafted, however, it could seriously impede international trade, product development, technology transfer, and scientific research. Potential benefits could also be significantly offset by huge costs, uncertainty, and delays. Protocol development is proceeding rapidly; negotiations will be completed in February 1999.

Background: The Biosafety Protocol (BSP) is an outgrowth of the Convention on Biological Diversity (CBD), a multilateral treaty for protecting biodiversity. The CBD's sound and commendable goals are to: Conserve biodiversity and provide for its sustainable use, and promote the fair and equitable sharing of benefits derived from the genetic resources inherent in biodiversity.

A Biosafety Working Group (BSWG) was established under the CBD to draft a Protocol dealing with the " transfer, handling and use of 'living modified organisms' (LMOs) derived from biotechnology that may have an adverse effect on the conservation and sustainable use of biodiversity." The BSWG is negotiating aspects of the BSP, including Protocol scope, advanced informed agreements for shipments of LMOs, risk assessment parameters, liability, labeling, confidentiality, status of non-Parties to the treaty, and the relationship of the BSP to other international agreements. The CBD website (www.biodiv.org) contains detailed information on the CBD and BSP.

Protocol Scope: The BSWG is currently considering which materials, genetic modification techniques and activities the BSP will cover. Many Parties favor expanding the scope beyond organisms that may have an adverse effect on biodiversity to include most, and perhaps all, LMOs. Others want to expand the scope even further to include products derived from or produced by LMOs. If this approach is accepted, the BSP would cover bulk commodity grains, raw and processed foods and food ingredients, animal feed, and pharmaceuticals. Covered products of biotechnology will likely include most genetically modified organisms, including modified cells and seeds, and may also include: products derived from or produced by genetically modified organisms/cells/seeds or vectors and plasmids used to create genetically modified organisms/cells/seeds. There are many methods for "altering the genetic material in a way that does not occur naturally," some of which have been used for decades. The methods of genetic modification covered by the BSP, which are still under debate, will include recombinant DNA techniques and direct injection of nucleic acids into cells and may also include cell fusion and other genetic modification techniques. Therefore, LMOs genetically modified using any of these techniques and products derived from those LMOs may be captured.

Activities covered by the BSP will include transboundary movement and deliberate releases, and may also include handling, transfer and use of genetically modified organisms, including contained uses. Key Requirement: According to current language in the negotiating text, shipments of products captured by the provisions would require an explicit advanced informed agreement (AIA) between the exporting and importing country before the product can be shipped. The exporter would provide a written notification of shipment, accompanied by an extensive risk assessment, to the importer. The time frame for accepting or rejecting the shipment is unclear, but could be as long as 6 months or even undefined.”

#### CBD solves biotech research, agriculture, burden sharing, and biodiversity

BIO 22(Biotechnology Innovation Organization, BIO is the world’s largest advocacy association representing member companies, state biotechnology groups, academic and research institutions, and related organizations across the United States and in 30+ countries, “The Biosafety Protocol-An Overview”, <https://archive.bio.org/articles/biosafety-protocol-overview>, Accessed June 19, 2022)//AS

“Desired Outcomes Biodiversity is a global resource of tremendous value to all of humankind. The CBD provides an important opportunity for nations to work together on an issue vitally important to us and future generations. To that end, we support a BSP that furthers the goals of the CBD: The conservation and sustainable use of biodiversity and equitable sharing of the benefits of biotechnology. To contribute to these goals, the BSP must: Be based on sound scientific principles. Take into account the actual environmental risks and the benefits of biotechnology, especially its role in facilitating biodiversity conservation. Focus on the transboundary movement of LMOs that may threaten biodiversity. Not unnecessarily restrict the transboundary movement of LMOs that pose no threat to biodiversity, thus increasing costs and delays without compensatory increases in environmental protection. Be consistent with existing international obligations to protect the environment. Encourage technology transfer and information sharing so all countries can benefit from advances in medical, agricultural and environmental biotechnology, while, at the same time, allowing for the protection of confidential information and intellectual property. Not divert resources from the protection of biodiversity to the development and administration of a regulatory system requiring case-by-case review of low-risk products. Be flexible so that any country can respond rapidly and appropriately to favorable developments in the new and evolving field of biotechnology.”

### 2NC --- Modelling

#### CBD and BSP bolsters biotechnology trade and co-research and increases unity between countries

UNEP 10 (UNEP Convention on Biological Diversity, The conservation of biological diversity, The sustainable use of the components of biological diversity, The fair and equitable sharing of the benefits arising out of the utilization of genetic resources, “United Nations Decade on Biodiversity”, 2010, <https://www.cbd.int/undb/media/factsheets/undb-factsheets-en-web.pdf>, Accessed June 18, 2022)//AS

The reason for this market failure is simple: most biodiversity components are considered ‘public goods’, belonging to everyone and to no one. Consequently, there is little concern in economic decision-making for their conservation and sustainable use. The economic work under the Convention on Biological Diversity seeks to elucidate this ‘hidden’ economic value of ecosystem services and the underlying biodiversity and incorporate it into market prices through the use of incentive measures that favour the conservation and sustainable use of biodiversity. “Work under the Convention, in partnership with the World Trade Organization, also looks at the relationship between its provisions and international trade rules. This is part of a broader effort by the international community to ensure harmony and mutual support between international trade rules and international environmental law, in order to both maintain biodiversity and promote international trade for the common goal of sustainable development. An important= goal of the Convention is that no species of wild flora and fauna should be endangered by international trade hence the CBD is closely cooperating with the Convention on International Trade in Endangered Species of Wild Fauna and Flora.”

#### CBD gives incentives for follow on that they can’t access.

UNEP 10 (UNEP Convention on Biological Diversity, The conservation of biological diversity, The sustainable use of the components of biological diversity, The fair and equitable sharing of the benefits arising out of the utilization of genetic resources, “United Nations Decade on Biodiversity”, 2010, <https://www.cbd.int/undb/media/factsheets/undb-factsheets-en-web.pdf>, Accessed June 18, 2022)//AS

“Biodiversity is the basis for ecosystem services, which are essential for human well-being and economic development. In addition to its intrinsic value, biodiversity and ecosystem services are therefore also of tremendous economic value. However, many ecosystem services are not traded on markets and their value is not properly reflected in existing market prices for other goods and services. Markets, when left alone, do not tell the ‘ecological truth’ and will therefore provide insufficient, if any, incentives to individuals, companies and governments to use biodiversity, and related ecosystem services, in a sustainable manner. The reason for this market failure is simple: most biodiversity components are considered ‘public goods’, belonging to everyone and to no one. Consequently, there is little concern in economic decision-making for their conservation and sustainable use. The economic work under the Convention on Biological Diversity seeks to elucidate this ‘hidden’ economic value of ecosystem services and the underlying biodiversity and incorporate it into market prices through the use of incentive measures that favour the conservation and sustainable use of biodiversity.”

#### Protocol increases trade and international cooperation

BIO 22 (Biotechnology Innovation Organization, BIO is the world’s largest advocacy association representing member companies, state biotechnology groups, academic and research institutions, and related organizations across the United States and in 30+ countries, “The Biosafety Protocol-An Overview”, <https://archive.bio.org/articles/biosafety-protocol-overview>, Accessed June 19, 2022)//AS

“THE PROPOSED BIOSAFETY PROTOCOL: KEY ISSUES The Parties to the Convention on Biological Diversity intended for the Biosafety Protocol to govern the transboundary movement of Living Modified Organisms (LMOs) that may have an adverse effect on the conservation and sustainable use of biological diversity. Jakarta Decision II/5, which established the negotiating parameters, provides that the Protocol: Not exceed the scope of the Convention; Not override or duplicate any other international legal instrument; Not unduly hinder access to and transfer of technology, and Be efficient, effective and minimize unnecessary negative impacts on biotechnology research and development. To serve the goals of the Convention and meet the conditions specified by Decision II/5, the Protocol must provide for the conservation and sustainable use of biological diversity, while at the same time allowing for the development and use of valuable new products. It must also be consistent with other international agreements and not cause unwarranted disruptions in the transboundary movement and trade of essential materials. To meet these objectives we recommend that the Biosafety Protocol be built on the following key positions: The scope of the Protocol must govern only those LMOs and intended uses that may have a significant adverse effect on biodiversity. Extending the scope of the Protocol cover LMOs and intended uses that, based on scientific principles, will not have significant adverse effects on biodiversity would impede access to agricultural, medical and other beneficial products without a compensatory increase in biodiversity protection. LMOs and intended uses that realistically will not have adverse effects on biodiversity should not be included in the scope of the Protocol. This will allow resources to be focused more effectively. Appropriate exclusions include, at a minimum, LMOs that have been reviewed and accepted for commercial or research use by the importing country; LMOs destined for contained use or transport; commodities approved for commercialization, and pharmaceuticals. The Advanced Informed Agreement (AIA) procedures should be applied only to those LMOs and intended uses that may realistically have a significant adverse effect on biodiversity. A "Notice of First Shipment" should be the primary mechanism to inform countries of the proposed shipment of an LMO. An AIA provision that requires written notification and consent for all LMOs will be extremely costly, demanding and burdensome for governments to administer, especially as the number of shipments covered by the Protocol increases. Moreover, if an intricate, lengthy and repetitive AIA process is applied to all LMOs, access to food, fiber and health care products will be impeded as will the development of new products. The Protocol must be consistent with international trade rules. If the scope of the Protocol is unnecessarily broad and the AIA procedure is excessively burdensome, the Protocol could have serious negative impacts on the trade. As such, the Protocol's scope and AIA provisions must be limited to those LMOs and intended uses that may realistically have a significant adverse effect on biodiversity. The decision to approve or deny shipment of an LMO covered by the Protocol must be based on sound science regarding real or reasonably anticipated effects on biodiversity. Speculative, non-significant adverse effects on biodiversity must not be used to reject products. Discrimination of products based on their production techniques must also be avoided. The Protocol must provide for the protection of confidential business information and other intellectual property. The Protocol must contain clear and appropriate procedures for designating and protecting confidential information and intellectual property shared in conjunction with the notification provisions of the Protocol. Procedures for resolving disputes over confidentiality claims regarding protected and privileged information must also be defined in the Protocol. In the absence of protection afforded by such procedures, companies and institutions will be reluctant to engage in commercial trade, international product development or exchange of research materials involving LMOs covered by the Protocol. The Protocol should not create an international system of liability. Existing national and regional legal systems should be relied upon to determine what triggers legal liability for harm to biodiversity, the nature and extent of harm that can be compensated, and the procedural system to obtain relief from liable parties.”

### 2NC --- Solves

#### Biosafety protocol solves regulations and safety without disrupting innovation.

IATP 00 (Institute of Agriculture and Trade Policies, advocate for policy in the public interest at the state, federal and international level striving for research, collaboration, and policy change, “Global Industry Coalition - Biotechnology - Industry Leaders Support Safety Protocol Workable Agreement Vital to Future of Biotechnology”, January 14, 2000, <https://www.iatp.org/news/global-industry-coalition-biotechnology-industry-leaders-support-safety-protocol-workable-agree>, Accessed June 19, 2022)//AS

“MONTREAL - The Global Industry Coalition continues to support a practical and workable Biosafety Protocol that would share the benefits of biotechnology, while protecting and sustaining biological diversity. The Global Industry Coalition pledges to support efforts to achieve a successful outcome to the Biosafety Protocol negotiations in Montreal, January 24-28. The Coalition represents more than 2,200 companies from more than 130 countries. "The nations participating in this international negotiation cannot settle for anything less than a Protocol that is practical and workable," said Joyce Groote of BIOTECanada, chair of the Global Industry Coalition. "We hope for success in Montreal but these matters are too important for us to do anything other than keep working until we achieve a practical and workable Protocol." Essentially, a Biosafety Protocol should create a scientifically-based framework that will facilitate international commerce as well as co-operative research and development in biotechnology among all countries. Biotechnology enables all countries to share the tools that can improve agricultural production, enhance the nutritional benefits of food, protect the environment and generate breakthroughs in health care and renewable fuels. In the past five years, considerable progress has been made through international negotiations for a Protocol. This follows through on the commitments made at the 1992 Earth Summit in Rio de Janeiro, where countries agreed to better stewardship of our planet. The Coalition has been fully supportive and involved in this process. Working under the auspices of the United Nations, delegates attending the Biosafety Protocol negotiations must endeavour to find a realistic balance that will protect biodiversity without disrupting research, innovation and trade. While the meeting is intended to produce an agreement that can be adopted in Montreal, the Coalition members, as responsible corporate citizens, expect the dialogue to continue until there is a satisfactory, workable Biosafety Protocol.”

#### Convention on Biosafety Protocol and Biosafety program allows for concrete biodiversity protection to take place

UNEP 10 (UNEP Convention on Biological Diversity, The conservation of biological diversity, The sustainable use of the components of biological diversity, The fair and equitable sharing of the benefits arising out of the utilization of genetic resources, “United Nations Decade on Biodiversity”, 2010, <https://www.cbd.int/undb/media/factsheets/undb-factsheets-en-web.pdf>, Accessed June 18, 2022)//AS

“The Convention on Biological Diversity (CBD) is an international legally-binding treaty with three main goals: conservation of biodiversity; sustainable use of biodiversity; and the fair and equitable sharing of the benefits arising from the use of genetic resources. Its overall objective is to encourage actions which will lead to a sustainable future. The conservation of biodiversity is a common concern of humankind. The CBD covers biodiversity at all levels: Ecosystems, species and genetic resources. It also covers biotechnology through the Cartagena Protocol on Biosafety. In fact, it covers all possible domains that are directly or indirectly related to biodiversity and its role in development, ranging from science, politics and education to agriculture, business, culture and much more. The governing body of the CBD is the Conference of the Parties (COP). This ultimate authority of all governments (or Parties) that have ratified the treaty meets every two years to review progress, set priorities and commit to work plans. In 2010, Parties to the CBD adopted the Strategic Plan for Biodiversity 2011–2020, a ten-year framework for action by all countries and stakeholders to safeguard biodiversity and the benefits it provides to people. The Secretariat of the Convention on Biological Diversity (SCBD) is based in Montreal, Canada. Its main function is to assist governments in the implementation of the CBD and its programmes of work, to organize meetings, draft documents, and coordinate with other international organizations and collect and spread information. The Executive Secretary is the head of the Secretariat.”

#### CBD solves by using the treaty as a tool in legislative committees.

Chandra 11 (Alvin Chandra and Anastasiya Idrisova, School of Earth, Atmospheric and Environmental Sciences, The University of Manchester, Oxford Road, Manchester and Department of Environmental Sciences and Policy, Central European University, Nador Utca, Springer Science+Business Media, “Convention on Biological Diversity: a review of national challenges and opportunities for implementation”, September 23, 2011, <https://www.researchgate.net/profile/Alvin-Chandra-2/publication/257538222_Convention_on_Biological_Diversity_A_review_of_national_challenges_and_opportunities_for_implementation/links/578f098908aecbca4caadb0c/Convention-on-Biological-Diversity-A-review-of-national-challenges-and-opportunities-for-implementation.pdf>, Accessed June 18, 2022)//AS

“The ultimate conservation challenge for all the countries remains halting biodiversity loss. This review however reveals that developing and developed countries and transition economies are at different stages of implementing the different requirements of the CBD. The countries that have progressed most on the programmes of work of the CBD also have developed economies and strong capacity to share information, coordinate stakeholder actions, and apply economic incentive measures. Developing countries and transition economies however are in the process of implementing measures on capacity development, awareness-raising, engaging key sectors and stakeholders, and mainstreaming of biodiversity targets. Additional efforts are required by developing countries and transition economies on knowledge and information-sharing mechanisms, engaging indigenous communities and developing sustainable financing mechanisms for conservation. The key challenges to the national implementation of the CBD identified in this research can be major explanations of failure to achieve the 2010 Biodiversity Targets. National challenges are complexed by multiple interactions with political, societal, legal, economic policy, and financial factors. The underlying, persisting problem is that limited capacity in developing countries and transition economies undermines conservation initiatives. This study is also of the view that the CBD objectives and targets cover an enormous range of tasks and agendas for the Parties, which can create confusion and divert attention from issues most pertinent to biodiversity conservation at the national level. This is particularly relevant for issues on access and benefit sharing, indigenous rights, traditional knowledge, and technology transfer, where gaps still remain within national legislations and the CBD. Despite many challenges, institutions, stakeholders, and the Parties have demonstrated certain best practices and developed networks of inquiry for CBD implementation. This study proposes the following recommendations for inclusion in national strategies to address the challenges and achieve the Convention’s objectives: • Institutional and capacity: Implementing the NCSA priorities and reviewing existing regulatory processes, including creating incentive schemes for skilled practitioners to engage in the biodiversity conservation field. • Knowledge and accessible information: National agencies should develop communication strategies and make information available online through user-friendly and contemporary websites that provide key audiences the ability to take relevant action. • Economic policy and financial resources: Developing and marketing quality biodiversity projects through a resource mobilisation strategy. Market-based instruments such as payments for ecosystem services and fair trading schemes should be designed, piloted and where possible, replicated to stimulate sustainable financing schemes. • Cooperation and stakeholder involvement: Consulting key stakeholders and the community to better understand their problems and opportunities, and support mutual actions on conservation. Developing and formalising partnership initiatives with the scientific community will also actively promote joint actions. • Mainstreaming and integration of biodiversity: Engaging national planners, statisticians and finance staff for setting national targets and allocating direct budgetary support for CBD implementation. Lessons learnt from mainstreaming initiatives in successful countries are useful, which can be documented and disseminated to other Parties. It is also important to point out that national conservation measures should be supported by multiple sectors and secure high level political support. Political, economical, and legislative sectors are more likely to show interest in CBD implementation and use it as a tool for managing biodiversity when they know the Convention processes and perceive it as a benefit. Modest investments in capacity building and training, and engaging different sectors in setting priorities would have a significant pay-off.”

## Funding

Military funding for brain health projects

Macaulay 21 [Thomas; 10/5/21; City University London Master’s Degree ; “US Army funds ‘sleeping cap’ that could modulate brain health of soldiers,” <https://thenextweb.com/news/us-army-funding> sleeping-cap-that-modulates-soldiers-brain-health]

After experimenting with exoskeletons, performance-enhancing drugs, and AR goggles to develop super soldiers, the US military has taken a punt on a brain-modulating skullcap. The army has issued funding for a wearable device that analyzes how the brain disposes of waste during sleep. The system will be developed by researchers at Rice University, Houston Methodist Hospital, and Baylor College of Medicine. Ultimately, the team wants to create a headset that can treat sleep disorders in real-time. But first, they aim to track and adjust the flow of cerebrospinal fluid as it flushes waste out of the brain. Currently, this is done with magnetic resonance imaging equipment. Paul Cherukuri, executive director of Rice’s Institute of Biosciences and Bioengineering, said the Pentagon wants to create a more compact alternative: Since an MRI can’t be easily transported, the Department of Defense asked if we can design a small, portable cap that can measure and modulate the brain health of warfighters during sleep to enhance their performance. Developing this prototype will require us to start with off-the-shelf devices and learn from them in parallel with building our own sensor technology and algorithms at Rice. The final device could merge multiple streams of data through machine-learning software to give clinicians a real-time view of the brain-clearing in action. The team aims to have preliminary results of their project within a year. The project could support new treatments of brain disease, but it also evokes terrifying visions of unsleeping super soldiers.

### 1NC --- Private Sector

#### Funding through startups solve and uses fewer government resources

Chen 21 [Jenny ; 8/21/21; Harvard Medicine and MIT Graduate ; “Fundraising in Bioprinting: 3DHEALS Perspective – Guide,” <https://3dheals.com/fundraising-in-bioprinting-3dheals-perspective-guide/>]

Where to find funding for early-stage bioprinting startups?

While a frothy market may not be good news to investors, investing in the right startup even at a higher valuation is still the winning move.

On the other hand, to the entrepreneurs in bioprinting, biotechnology, and life sciences, the timing could not be better. Nonetheless, for scientists turned into first-time entrepreneurs, it is still hard to figure out where to find early-stage funding, and how to fundraise in general.

Early 2021, I have summarized a number of notable companies in the space of healthcare 3D printing, ranging from new startups (“newborns”) to new public offerings (SPAC or IPO, “unicorns”). It is often insightful to observe companies at different stages throughout their life cycle, find parallel storylines in the public market, and figure out the best strategies to fundraise or to invest. Often, reading the S1 of similar pre-IPO companies can be helpful in either polishing up a startup’s pitch deck or for investors interested in early-stage startups.

In general, there are 7 major funding sources. In the order of increasing difficulty and larger amount, they are:

Grants and prizes (Free money!)

Friends and family/angel investors

Investment banker/Business loans

Crowdfunding (Regulation CF)

Accelerator/Incubator

Corporate VC

Venture Capital

Grants and Prizes – Free $$$

Grants and prizes are excellent non-diluting funding, but are they really free?

There is no free lunch, and that still stays true.

The other prized possession of the founders is Time, and applying and waiting for this nondiluting funding takes a lot of time especially when the grant/prize amount is small relative to the fundraising goal. Typically these make a lot of sense for seed-stage biotech companies, which need 1-5 million USD. There are many additional benefits in getting grants. To save more time, some companies may consider hiring a specialist dedicated to writing grants. They are not just for non-profit organizations.

However, for series A, the amount increases to double-digit millions in USD, and anything beyond will be into the triple-digit territory. Grants and prizes opportunities that would satisfy these dollar amounts are increasingly scarce as the amount increases.

I also don’t know of any company that has ever successfully exited due to free money alone. More importantly, since this is a business, you would want market validation, and that’s why raising institutional funding will be important beyond just the dollar amount.

Additionally, government grants (at least in the United States) are not given without caveat. There are occasions when IP generated under government grants is subject to certain rules and restrictions. Weighing the cost and benefit with your patent lawyer will be a wise move before your grant strategies.

Friends, Family, Angel Round

Angels play a significant role in funding early-stage startups, especially for first-time entrepreneurs with no track record of building businesses or even telling a good story around his/her company. “The best available estimates are that about 300,000 people have made an angel investment in the last two years. Many more people could become angels based on a net worth of $1 million or more, the potential number of angel investors is 4 million.”[Ref 4] Some angel investors invest in the founder’s character/talent through their personal interactions, some invest in the company’s story, and others invest for impact. If a startup can curate a good group of angel investors, sometimes, this can be equivalent to having a great group of advisors, marketing, future fundraising channels, in addition to the checks they write. While a typical angel check size (5K-100K) is insufficient for a seed round for bioprinting startups, angel groups can often provide amounts in millions.

While friends-and-family round sounds warm and cozy, I would advise caution, that is, if you want to keep those same friends and family. The bottom line is that if those friends and family members are also angel investors in other companies, chances are they are more knowledgeable in terms of the risks involved. That is, 80% of all startups will fail in five years.

With the newly instituted Regulation CF, many platforms now provide crowdfunding opportunities that allow non-accredited investors to invest as low as 100 dollars. This method can be particularly helpful for a seed round or bridge round when data is too scarce for institutional investors. We will expand on these platforms and the regulations around them in a later blog post.

Institutional Investors

But since biotechnology companies often need significantly larger check sizes and longer runways to achieve the holy grail, such as bioprinting organs, raising institutional money is almost inevitable. But what if you don’t know of any institutional investors?

There are generally three categories where you can find them:

Accelerator/Incubators

Corporate VC

VC

One way to figure out who you should approach for fundraising is through reverse engineering. Some of the investor information is held private, but much of this information is public information. You can find this information from many different data aggregators such as Crunchbase or Pitchbook (expensive!).

For example, if you are a bioink startup and are looking for VCs, you could find existing similar biomaterials or bioink companies in the market (large or small), and then figure who their investors are. Large chemical companies often have a VC arm because they need innovations to stay competitive and are always looking out for potential acquisition deals. Therefore, by association, you can generate a few dozens of potential firms that you can reach out to that could be interested in investing in your company. A word of caution, however, is that VCs may have a conflict of interest in investing in too many startups that are direct competitors to one another.

How to get your foot into the door?

“Networking. Networking. Networking.”

This would be a learning process, and you are likely to make many mistakes. Your time is as valuable (if not more) as the investors’. The law of “Give and Take” is always in play in this most capitalistic process of startup fundraising. Always ask what kind of value any kind of interactions or transactions have returned to you or the investors. (No hard feelings if you have not responded to my emails lately…)

It is a tough job, but isn’t this adventure the exact reason you have abandoned your professorship in the ivory tower?

How to participate in Pitch3D?

Many moons ago, we have published a few blogs focusing on how to pitch in front of the investors, and they are still worth a read here:

Fundraising in Healthcare 3D Printing, Part I: So, You Want to Pitch?

Fundraising in Healthcare 3D Printing, Part II: Are you Printing Money?

Try to pitch to investors carrying lower stakes, for example, friends and family, Pitch3D, or any friendly angels (like myself). If you make a mistake with them, you can get their feedback to polish up your presentations for higher-stake investors. For those who are truly inexperienced, I would highly recommend reputable accelerators or incubators such as YCombinator, IndieBio, Techstars, among others. You lose a small percentage of equity for years of company-building experience, investor network, the reputation that would add valuation.

#### Even if years away, funding allows for fast development on Biotech.

Hanaphy 20 [Paul ; 5/28/20; Kingston University Masters degree ; “BRINTER RAISES €1.2M TO FUND LAUNCH OF SCALABLE BIOPRINTER IN NEW MARKETS,” https://3dprintingindustry.com/news/author/paul-hanaphy/]

Funding international growth According to Brinter, many researchers still use traditional drug discovery and disease modelling methods, when its proprietary 3D bioprinter could help scale the entire process. As a result, using its newly-raised funding, the company aims to make its technology as accessible as possible, and bring bioprinting within reach for all U.S. or European clinical firms, hospitals and universities. At present, Brinter’s clientele includes companies like Nanoform, as well as researchers at VTT, the University of Glasgow, Johannes Gutenberg University of Mainz, University of Oulu and University of Helsinki. In one particularly promising project at the University of Eastern Finland, the firm’s technology is currently being used to 3D print neural matter for future brain disease modelling applications. “I am extremely excited to continue our 3D brain printing project with Brinter,” explained Jari Koistinaho, Professor of Regenerative Medicine at the University of Eastern Finland. “3D bioprinting will soon provide us with fine-tuned human mini-brains and brain prosthetics, thereby deepening our understanding of the human mind and our ability to combat serious brain disorders.” For its part, Innovestor has also identified “accelerated technological, material and methodological” advances within the bioprinting industry, and it now anticipates that Brinter’s technology will supplement this trend, making scientific R&D up to ten times faster and helping to usher in the age of bioprinted heart/kidney transplants. “We are very excited to be a part of Brinter’s journey,” concluded Wilhelm Lindholm, CEO of Innovestor. “Brinter is an exciting addition to our portfolio as the company’s competitive advantages of multi-material printing capabilities, modularity, and scalability combined with their own easy-to-use software application were very convincing.” “COMPANIES LIKE BRINTER ARE PAVING THE WAY FOR 3D BIOPRINTING, REVOLUTIONIZING THE FUTURE OF MEDICINE TO THE POINT WHERE A CUSTOMIZED HEART OR KIDNEY CAN BE MADE FOR A TRANSPLANT PATIENT.” Advances in bioprinted organs While transplantable bioprinted organs remain years away from reality, recent advances in the technology may have shortened this wait considerably. 3D Systems’ continued interest in bioprinting will no doubt hasten its development, and the firm reported “tremendous progress” within its dedicated Print to Perfusion program earlier this year. As part of a strategic refocus announced by the company in 2020, it has also sought to build on its core healthcare and industrial segments, and acquired Additive Works and bioprinting firm Allevi during May 2021, with this in mind. Similarly, manufacturers such as UpNano are increasingly entering the bioprinting sector, and the company has now launched its own NanoOne Bio system. Released in May 2021, the firm’s machine is reportedly capable of constructing 3D tissues out of living cells, resulting in viable meso-to-nanoscale sized structures. In more experimental developments, the National Science Foundation (NSF) has awarded Allegro 3D nearly $1 million to fund the R&D of its novel high-throughput bioprinting platform. Using the capital, the firm aims to create a machine that’s capable of rapidly producing in-vitro therapeutic and biomedical testing models.

### 2NC --- Funding Solves

#### **Venture Capital funding allows R&D and creates jobs helping economy**

PHRMA No Date [National Institute Health; trade group representing companies in the pharmaceutical industry in the United States.; “RESEARCH & DEVELOPMENT

Venture Capital ,” https://phrma.org/policy-issues/Research-and-Development/Corporate-Venture-Capital]

The U.S. biopharmaceutical ecosystem has propelled the U.S. to global leadership in medical development. Here we look at the impact of venture capital and small startup companies in this process from 2000-2017.

The vast majority of biopharmaceutical companies are small startups working to turn the latest scientific discoveries into viable treatments for a whole host of diseases and medical conditions. Thousands of these companies – which are found in almost every state in the U.S. – operate without profits or even revenues, yet are able to devote substantial resources toward their research and development efforts. This would not be possible without the venture capital investors who provide the necessary backing for biopharma startups to operate during the long research and development time frame for biopharmaceuticals. Indeed, it would be virtually impossible for biopharma startups to ever get off the ground without the investment of time, resources and guidance that their venture partners provide. The corporate venture capital arms of established biopharmaceutical companies – particularly PhRMA member companies – provide a considerable share of these inputs.

New medicines developed by startups not only advance science and human health but also bring jobs and economic growth to their communities. While relatively small in numbers compared to large firms, jobs in startup biopharma companies are knowledge-intensive and high-impact, generating a positive ripple effect throughout the regional economy. In this way, venture-backed enterprises deliver the dual benefits of scientific advancement and economic growth beyond the traditional biopharmaceutical hubs into smaller communities across the nation.

### 2NC --- Bioprinting

#### Bioprinting is costly but funding allows development to proceed.

Hanaphy 20 [Paul ; 5/28/20; Kingston University Masters degree ; “BRINTER RAISES €1.2M TO FUND LAUNCH OF SCALABLE BIOPRINTER IN NEW MARKETS,” https://3dprintingindustry.com/news/author/paul-hanaphy/]

Finland-based 3D bioprinting start-up Brinter has revealed that it has received €1.2 million worth of investment. Raised via a seed funding round led by early-stage VC firm Innovestor, the capital is set to be used as a means of expanding the company’s operations, allowing it to more easily address the U.S. and European medical markets with its modular 3D bioprinter, which it says could have future organ fabrication applications. “Bioprinting can rapidly unlock the opportunities behind long-running but unrealised science and research, and plays a key role in pushing the frontier of medical science,” said Tomi Kalpio, CEO of Brinter. “This will result in an improved quality of life for patients through the expansion of more personalised treatment and the ongoing development of bioprinted ‘spare parts’ that can save lives.” “WE ARE EXCITED TO HAVE THE BACKING OF INNOVESTOR, WHO CAN HELP US ACCELERATE THE DEVELOPMENT OF OUR OPERATIONAL CAPABILITIES AND SCALE IN NEW GEOGRAPHIES.” Brinter’s bioprinting technology Based in the Finnish city of Turku, and spun-off from the 3D printing bureau 3DTech Ltd, Brinter develops bioprinting systems, modules and inks for medical, research and cosmetics clients. The firm’s offering revolves around its aptly-named ‘Brinter 1,’ which is capable of depositing layers of cell-laden hydrogels into oncological models as well as cancerous and cartilage microtissues. In practise, Brinter clients are able to use the company’s software to turn MRI, X-ray or CT scanning data into CAD models, before printing them into viable soft tissues for use within drug evaluations, in a way that could help accelerate the translation of new medicines into clinics and bring an end to the use of animal testing. Priced at €24,900, Brinter’s machines are far from cheap, but they are also uniquely modular in that users can acquire and add different printheads to access a variety of modalities on a single platform. The company’s Pneuma Tool, for instance, enables the dispensing of low-to-medium viscosity bio-inks, while its premium Visco Heated Tool comes with material temperature-regulating functionality.

## Pharma

### 1NC --- Vaccines

#### Vaccine development solves emerging diseases

PHRMA 22 [National Institute Health 4/?/2020 ; trade group representing companies in the pharmaceutical industry in the United States.; “New Era of Medicine: Vaccines,” https://www.phrma.org/science/new-era-of-medicine-vaccines]

Vaccines represent some of the most impactful public health advances seen to date, playing a critical role in reducing the spread of, and, in some cases, eliminating the threat of the world’s many devastating infectious diseases.

The human immune system is incredibly powerful and versatile, working continuously to keep a variety of invaders from causing infection and disease. From bacteria, to viruses, to parasites, the immune system recognizes invading threats and triggers a response in the body to contain and combat invaders. And although the immune system is incredibly robust, it is not invincible which is why vaccines are needed to help support the body’s defenses.

Vaccines present a number of unique challenges that make them particularly complicated to research, including scientific, clinical and logistical hurdles throughout the development process. These challenges are made more difficult during public health emergencies. Even with these challenges, some of the newer types of vaccines have the potential to move faster from initial virus identification to a viable vaccine, and faster from there to a licensing application and manufacturing scale up.

### 2NC --- Follow on

#### US Is a hotspot for Biopharmaceuticals leaders

BioSpace 22 [BioSpace Editorial Staff 9/21/2020 ; The Home of the Life Sciences Industry. Find biotech, clinical research and pharmaceutical jobs from thousands of employers; “Investment in Biopharma is Reaching an Inflection Point,” https://www.biospace.com/article/investment-in-biopharma-is-reaching-an-inflection-point-/]

In particular, America’s east coast hubs excel due to an enviable university system, innovative biotech companies and the presence of large pharma companies like Pfizer, Johnson & Johnson and Merck & Co. Adding to the allure are plentiful enterprise partnerships, a robust entrepreneur ecosystem and a well-functioning incubator system.

New Jersey leads the nation in big names. There are 139 U.S. Food and Drug Administration-registered biopharmaceutical manufacturing facilities in the state, and 25% of all cell and gene therapies are being developed there. Among the largest biopharma companies in the country, 13 are in New Jersey, along with 3,280 life science establishments. More than 50% of all new FDA novel medicines approved in 2019 were from companies with a footprint in New Jersey.

New York, home of Pfizer and Bristol Myers Squibb is ranked second in the nation for bioscience jobs. A $1.8 billion expansion in Tarrytown, NY by Regeneron Pharmaceuticals announced mid-July is set to add 1,000 jobs over the next five years, with the company also adding to its research, preclinical manufacturing and support facilities.

What New Jersey is to big pharma, the same can be said of Massachusetts when it comes to biotech. In 2020, biopharma employment grew by 5.5% to about 85,000 jobs, and the state’s industry raised $5.8 billion in venture capital.

Over the past 15 years, Massachusetts has seen a 92% increase in biopharma employment, Massachusetts Biotechnology Council said in its latest industry snapshot.

MassBio said the record-breaking rates at which Massachusetts-headquartered firms are raising VC funds is leading to “incredible growth in the real estate pipeline to meet the demand of biopharma companies that are choosing to launch and scale across Massachusetts.”

One such company, Nuvalent, launched with $50 million in Series A financing from Deerfield Management to develop innovative small molecule kinase inhibitors for programs in non-small cell lung cancer (NSCLC)

The Boston metropolitan area, and in particular Cambridge, seems to be holding its own as the pre-eminent biotech hub in the world. At the end of August, biotech start-up Laronde raised $440 million in a Series B round. Laronde is creating endless RNA, a novel, engineered form of RNA that is programmable to express therapeutic proteins to the human body.

Biogen and Vertex are the largest biopharma employers in Massachusetts, followed by Moderna.

In addition, seven Korean pharmaceutical and biotech companies have recently moved into the Cambridge Innovation Center to expand their reach into the U.S.

Eager to grab some of the action, Texas is determined to plant its flag as the next US biotech hub. Oncology leads the way here, with over 4,700 drug indication programs under development, equal to 71% of all global pipelines. Emerging biopharmas' pipelines are robust here, ranging from start-up to mature, according to a recent BIO Industry analysis.

### 2NC --- Vaccines

#### Developing vaccines is safe and effective

PHRMA 22 [National Institute Health 4/?/2020 ; trade group representing companies in the pharmaceutical industry in the United States.; “New Era of Medicine: Vaccines,” https://www.phrma.org/science/new-era-of-medicine-vaccines]

Vaccine Safety

Vaccines undergo a rigorous research and development process in order to ensure safety and efficacy, and continue to be monitored long after U.S. Food and Drug Administration (FDA) approval. Manufacturers and health authorities coordinate to ensure strict manufacturing and delivery schemes, in order to guarantee the quality and purity of vaccines. Data show that the current U.S. vaccine supply is the safest in history, due in part to the U.S. Centers for Disease Control and Prevention’s (CDC’s) long-standing vaccine safety program, which closely and constantly monitors the safety of vaccines. One important element of the program, the Immunization Safety Office, monitors possible vaccine side effects and works with public health stakeholders to assess possible connections to vaccines. For example, while some have had concerns that autism spectrum disorder might be linked to the vaccines children receive, studies have shown that there is no link between receiving vaccines and developing autism spectrum disorder.

Biopharmaceutical Companies continue to do R&D on vaccines

Powaleny 22 [Andrew 4/23/2020 ; Senior Director of Public Affairs at PhRMA and leads the organization's scientific communications, national advocacy events and grassroots initiative, Voters for Cures..; “New report shows nearly 260 vaccines in development, including dozens for COVID-19,” https://catalyst.phrma.org/new-report-shows-nearly-260-vaccines-in-development-including-dozens-for-covid-19]

There are several notable success stories in prevention of infectious diseases in the U.S. and worldwide. Smallpox at one point was one of the deadliest diseases in existence. But as a result of American immunization efforts, the last natural outbreak occurred in 1949. And across the globe due to aggressive vaccination programs naturally-occurring smallpox was declared eradicated in 1980. Though many diseases remain threats around the world, vaccination requirements in the U.S. have led to the elimination of once highly contagious infections impacting children, including polio in 1994, measles in 2000 and rubella in 2004.

In the United States today, 16 diseases are now preventable as a result of childhood vaccines, and routine immunization of U.S. children born between 1994-2018 has prevented more than 419 million illnesses.

Today, biopharmaceutical companies are working with stakeholders across the research and development (R&D) ecosystem to develop new ways of preventing and treating illnesses with innovative vaccines. According to a new report, there are currently 258 vaccines in development for the treatment or prevention of disease.

Among the vaccines in development are:

108 vaccines for cancer, including a therapeutic vaccine for non-small cell lung cancer, which uses messenger RNA to mobilize the patient’s own immune system to fight the tumor(s)

125 vaccines for infectious diseases, including a vaccine designed to prevent HIV infection by teaching a patient’s immune system to recognize and effectively fight the virus

14 vaccines for allergies, including vaccines that target peanut allergies

2 vaccines for Alzheimer’s disease, including one therapeutic vaccine that targets amyloid beta protein, which is linked to the development of the neurological disorder

#### 260 vaccines currently being developed now

PHRMA 22 [National Institute Health 4/?/2020 ; trade group representing companies in the pharmaceutical industry in the United States.; “New Era of Medicine: Vaccines,” https://www.phrma.org/science/new-era-of-medicine-vaccines]

As of April 2020, there are nearly 260 vaccines in development by America’s biopharmaceutical companies to both prevent and treat diseases including cancer, Alzheimer’s disease, allergies and autoimmune disorders. These vaccines offer significant hope for the future, with many vaccines in the pipeline using new technologies that have the potential to prevent the transmission of the human immunodeficiency virus (HIV), protect against malaria and even therapeutic vaccines to treat several types of cancer.

### 2NC --- Solves Cancer

#### Cancer treatment vaccines being developed

BioSpace 22 [BioSpace Editorial Staff 9/21/2020 ; The Home of the Life Sciences Industry. Find biotech, clinical research and pharmaceutical jobs from thousands of employers; “Investment in Biopharma is Reaching an Inflection Point,” https://www.biospace.com/article/investment-in-biopharma-is-reaching-an-inflection-point-/]

A Focus on Cancer Treatment

It is oncology that continues to dominate financings through later-stage deals. Cancer therapeutics were among the top indications with Series A funding, with 25 deals valued at $497 million sealed during the first half of 2020. As for the full year 2020, 44 deals were struck at $1.3 billion, and the first half of 2021 accounted for 34 deals at $1.1 billion.

## UN

### 1NC --- UN Solves

#### The UN has already taken the lead against bioweapons.

UN 10 [United Nations 12/16/1971; The United Nations is an intergovernmental organization whose purpose is to maintain international peace and security, develop friendly relations among nations, achieve international cooperation, and be a center for harmonizing the actions of nations ; “Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction,” https://treaties.unoda.org/t/bwc]

The States Parties to this Convention,

Determined to act with a view to achieving effective progress towards general and complete disarmament, including the prohibition and elimination of all types of weapons of mass destruction, and convinced that the prohibition of the development, production and stockpiling of chemical and bacteriological (biological) weapons and their elimination, through effective measures, will facilitate the achievement of general and complete disarmament under strict and effective international control,

Recognising the important significance of the Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, signed at Geneva on 17 June 1925, and conscious also of the contribution which the said Protocol has already made and continues to make, to mitigating the horrors of war,

Reaffirming their adherence to the principles and objectives of that Protocol and calling upon all States to comply strictly with them,

Recalling that the General Assembly of the United Nations has repeatedly condemned all actions contrary to the principles and objectives of the Geneva Protocol of 17 June 1925,

Desiring to contribute to the strengthening of confidence between peoples and the general improvement of the international atmosphere,

Desiring also to contribute to the realisation of the purposes and principles of the Charter of the United Nations,

Convinced of the importance and urgency of eliminating from the arsenals of States, through effective measures, such dangerous weapons of mass destruction as those using chemical or bacteriological (biological) agents,

Recognising that an agreement on the prohibition of bacteriological (biological) and toxin weapons represents a first possible step towards the achievement of agreement on effective measures also for the prohibition of the development, production and stockpiling of chemical weapons, and determined to continue negotiations to that end,

Determined, for the sake of all mankind, to exclude completely the possibility of bacteriological (biological) agents and toxins being used as weapons,

Convinced that such use would be repugnant to the conscience of mankind and that no effort should be spared to minimise this risk,

## Misc

### 2NC --- Super Soldiers

#### **The future of military enhancement with biotech is here to stay**

Malet 15 [David; 11/13/15; Qualifications; "Captain America in International Relations: the Biotech Revolution in Military Affairs," <https://www-tandfonline-com.proxy.lib.umich.edu/doi/pdf/10.1080/14702436.2015.1113665?needAccess=true>, IC]

On 27 August 2014, President Barack Obama unveiled the new ElectRx system, created by the Pentagon’s Defense Advanced Research Projects Agency (DARPA). Intended to preserve the health of United States military personnel and veterans, these “new computer chips [are] designed to modulate the nervous system to help with everything from arthritis to post-traumatic stress” (Lamothe 2014). While the exploits of superhero-like “metabolically dominant warfighters” may be more of a concern for moviegoers than military strategists today, biotechnologies are already being deployed to give the United States unprecedented strategic military advantage, and the effort and the billions of dollars of public funds invested in the furtherance of their creation merit examination. There has as of yet been little consideration in the international relations discipline of what the advent of augmented forces with unprecedented offensive and defensive capabilities mean for concepts of just war, or for the legitimacy that underpins the authority of successful international hegemonic actors. Yet, if past and recent developments in revolutionary new military technologies are any indication, debates about their deployment will inevitably arise. This article is not concerned primarily with the ethics of human enhancement, a literature which details the potential for social and economic improvement or inequality but neglects considerations of international security almost completely. Instead, it considers the import of biotechnologies that are currently at least being discussed as the basis of an effective combat capability of the future. These include physical and mechanical enhancements of troops that may be intended as purely defensive, but which also offer augmented offensive capability, and related ethical considerations, because they enable troops to securely project power in a way that no adversary would be able to match, belying any notion of a “fair fight.” Robbed of any hope of winning symmetrically, opponents would necessarily fall to strategies that would produce arms races or alternative disruptive technologies to compete. The character of Captain America, first introduced in comic books in March 1941, offers an easy shorthand for some of the technological innovations on the drawing board for twenty-first-century theaters of conflict. The early super-hero was physically enhanced by a combination of a “super-soldier serum” and “vita-rays,” but also provided with a unique indestructible shield that could also be used as an offensive weapon. He was therefore singularly both invulnerable and capable of projecting force in a way that no adversary could match, although the adversaries of the day soon developed their own special counter-forces in response. Potentially, some variation of this tale can be expected in coming decades, and indeed already began unmarked a decade ago in Iraq.

### 2NC --- Squo solves gene editing

#### **We’ve already banned gene editing.**

Kaiser 19 [Jocelyn; 6/4/19; Princeton University degrees in chemical engineering; “Update: House spending panel restoes U.S. ban on gene-edited babies,” https://www.science.org/content/article/update-house-spending-panel-restores-us-ban-gene-edited-babies]

\*Update, 4 June, 1:25 p.m.: By voice vote, the full Appropriations Committee of the U.S. House of Representatives today restored language to a 2020 spending bill that bars the U.S. Food and Drug Administration (FDA) from considering requests to approve any clinical trial "in which a human embryo is intentionally created or modified to include a heritable genetic modification." Late last month, an appropriations subcommittee had removed the rider, which has been part of the spending bill that funds FDA for the past 4 years. Today, Democrats who lead the spending panel said they had removed the rider because they wanted to spur a fuller debate on how the U.S. government should regulate the genetic modification of human sperm, eggs, or embryos. In particular, they said that although they support a ban on using gene-editing tools such as CRISPR to modify babies, they were concerned that the FDA rider might also hinder the development of potentially helpful therapies, such as modifying a cell's mitochondria to prevent heritable diseases. Several Democrats said they were reluctantly supporting the request from Republicans to restore the rider, and lawmakers from both parties suggested congressional health committees that shape agency policies need to address the issue comprehensively, rather than have it debated annually during the appropriations process.

Here is our previous story from 24 May:

A Democrat-led spending panel in the U.S. House of Representatives has dropped a provision that banned embryo editing with the intention of creating a baby. The draft bill is still moving through the legislative process, however, and Republicans will likely push to restore the language.

The ban was first added to the law that funded the U.S. government in 2016. It bars the Food and Drug Administration (FDA) from considering any clinical trial application "in which a human embryo is intentionally created or modified to include a heritable genetic modification." Although a different "rider" bars the National Institutes of Health from funding human germline editing—or the genetic modification of sperm, eggs, or embryos—such work is permissible with private funding. However, researchers would need FDA approval for a clinical trial.

A 2020 draft spending bill approved on 23 May by the House appropriations subcommittee that funds FDA does not contain the rider, as CQ first reported yesterday. A Democratic aide speaking on background told ScienceInsider: "The provision was dropped because it was inserted in private 3 years ago and has never been subject to public debate. We believe this provision could limit important scientific research and, if Congress chooses to prohibit such research, that should be done in the light of day."

The rider has served as a de facto U.S. ban on germline editing to create a baby, which is explicitly barred in some countries. Concerns about such experiments intensified in November 2018, when a Chinese scientist announced he had used the CRISPR gene-editing tool to modify the genome of twin baby girls in an effort to make them resistant to HIV. That work, which did not go through proper regulatory approvals in China and has been widely condemned as unethical, has drawn calls from some scientists and bioethicists for a global moratorium on human embryo editing.

But some scientific advocacy groups dislike the FDA bill language because it means Congress made the decision, not scientific and regulatory experts. Sean Tipton, chief advocacy, policy, and development officer at the American Society for Reproductive Medicine who is based in Washington, D.C., says the provision was "an antiscience rider." Removing it "allows the FDA to do its job."

Bioethicist Hank Greely of Stanford University in Palo Alto, California, agrees the language was "bad policy." He adds, "This is a good change, but it raises new challenges, for Congress and for society."

Dropping the provision frees FDA to consider allowing a less controversial approach that combines genetic material from a mother, a father, and an egg donor to prevent an embryo from inheriting a mother's mitochondrial disease, Greely notes. That "three-parent embryo" treatment is being tested in clinical trials in the United Kingdom and has been endorsed by U.S. experts. "It is much farther along … and U.S. clinical trials should not be under a blanket ban," Greely says.

The top Republican on the House appropriations agriculture subcommittee, Representative Jeff Fortenberry (R–NE), opposed removing the embryo editing ban. "Starting in 2016, the subcommittee acted to prevent an emerging science that would allow for the permanent modification of an individual's genetics and those of future offspring. This is a prohibition that is accepted by nearly every nation in the world due to the unknown risks," Fortenberry said.

The rider could still be added to the bill when it is taken up by the full House Appropriations Committee or when it reaches the House floor. The Senate has not yet crafted its version of the spending bill.

Correction, 4 June 2019, 2:52 p.m.: As the result of an editor's error, an update to this story incorrectly reported that the 4 June voice vote to restore the rider was unanimous. One Democrat, Representative Debbie Wasserman Schultz (FL), voted against restoring the rider.

#### China has already implemented gene editing regulations

Civil Code of The People’s Republic of China 20 [Civil Code of The People’s Republic of China; 5/28/20; Civil Code is expected to comprehensively strengthen the protection of people's various rights and improve the Chinese socialist system of laws adopted at the Third Session of the Thirteenth National People’s Congress; “Civil Code Of the People’s Republic of China,” http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf]

Article 1009 A medical and scientific research activity related to human genes, embryos, or the like, shall be done in accordance with the relevant provisions of laws, administrative regulations, and the regulations of the State, and shall not endanger human health, offend ethics and morals, or harm public interests.

Others have banned human gene editing

Laney 21 [Zhang; 2/26/21; foreign law specialist at the Law Library of Congress; “China: Multiple Areas of Criminal Law Changing under New Amendment,” http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf]

Crime of Implanting Gene-Edited Embryos into Humans

The amendment adds a new article 336a to the Criminal Law, creating a new crime of implanting gene-edited or cloned human embryos into human or animal bodies, or implanting gene-edited or cloned animal embryos into human bodies. The sentence is up to seven years in prison and a fine, if the circumstances are “especially serious.” (Amendment XI art. 39.)

# AFF

## Biotech

### 2AC --- Bans Fail

#### **Biotech in the military is inevitable.**

Malet ’11/15 [David; 11/13/15; Qualifications; "Captain America in International Relations: the Biotech Revolution in Military Affairs," <https://www-tandfonline-com.proxy.lib.umich.edu/doi/pdf/10.1080/14702436.2015.1113665?needAccess=true>, IC]

The Biotech Revolution in Military Affairs There have been numerous studies of the impacts of a wide array of emergent technologies by hegemonic actors or aspirants (For a preliminary list, see Jervis 1978, Levy 1984, Posen 1984, Shimshoni 1990, Arquilla and Ronfeldt 1997, Adams 1998, Murray and Millett 1998, Tannenwald 2008, Clarke and Knake 2010, Vogel 2012, Waltz and Sagan 2012, Carpenter 2013). However, there has been little examination of what the adoption of biotechnology by the leading military powers has meant or is likely to mean. The United States Office of Technology Assessment defines biotechnology as “any technique that uses a living organism, or parts of organisms, to make or modify products, to improve plants or animals, or to develop microorganisms for specific uses.” 320 D. Malet Other definitions include material patterned after living organisms but not necessarily using them as components (biomimetics). The conventional wisdom on biotechnology has held that coming decades will see Western nations increasingly vulnerable to ever-more sophisticated biological weapons attacks by non-state actors and rogue states. As recombinant genetic technology proliferates, a greater number of actors will possess genetic engineering capabilities that will enhance the lethality and durability of their biological weapons. Proponents of this perspective note that the overwhelming technological advantage in conventional forces enjoyed by the United States creates the incentive for competitors to develop effective asymmetric responses, and that the affordability, accessibility, and relatively easy preparation of biological weapons make them a likely means of doing so. In this view, the superior conventional capabilities of the US military not only fail to deter the proliferation of biological weapons, but encourage their development. Western states will face an increasing number of biologically armed opponents, and will remain on the defensive. The priority for military biotech research is therefore the development of protective equipment and vaccines, antibiotics and antivirals (Department of Defense 1998). However, this scenario requires the presumption that military applications of biotechnology will simply be a secular progression from the bacteriological warfare that has existed throughout history. Even when analysts have factored in the vast possibilities of genetic engineering, it has usually only been to the extent that they can breed deadlier pathogens, and that the growing availability of technology means that it may be used by a broader spectrum of actors. Conventional wisdom therefore predicts an unstable future for the international system, a Hobbesian world in which the weakest have power to kill the strongest. Rather than rogue states and non-state terrorists, it is the most powerful and resource-laden actors in the international system that will enjoy the advantages of “biological warfare” in the twenty-first century as they continuously integrate emergent biotechnologies into their military and national defense infrastructures and extend their dominance. This process will closely resemble the Revolution in Military Affairs (RMA) that occurred during the last 30 years of the twentieth century as the United States adapted its forces to exploit advances in new information technologies. The RMA, first described by the Soviet military intelligence in the 1970s and then witnessed by the world during the unexpectedly uneven 1991 Gulf War, occurred because the United States employed its competitive advantage in integrated computer systems. Rather than a single transformative device, like the atomic bomb, the steady accretion of advanced technologies augmenting existing equipment came to inform doctrine and strategies. The term asymmetric warfare is meant to describe efforts by weaker participants in military confrontations to frustrate the advantages of the stronger power by guerilla tactics or other unconventional methods not envisioned in force planning (Mack 1975). However, high technology also offers asymmetric advantages to the best-equipped actors, and American military planners sought to use the advances of the RMA to field forces that no state competitor could match. Their goals included “dominant maneuver” capability on the battlefield in bringing dispersed resources to bear against targets, “precision engagement” capability delivered by smart weapons, and “full dimension force protection” against all anticipated threats (Rizwan 2000). The ultimate expression of this vision would be a fighter comparable to a “Jedi knight” from the Star Wars films: a super-empowered solider, dressed in a protective stealth cloak and commanding an Defence Studies 321 armed companion drone, able to perform solo missions and to transmit data back to headquarters (Hundley and Gritton 1994). Coincidentally or not, this is precisely how Darth Maul was depicted in 1999’s The Phantom Menace. Military planners likewise foresee similar advantages conferred by developments across the various biotech fields. In coming decades, biotechnology is forecast to bring advances such as “rugged computers” made from biological components that will provide situational awareness to individual soldiers on the battlefield, camouflaged materials and lightweight armor incorporating the properties of living organisms, and ingested biological markers to distinguish friendlies, which would be of particular use in counterinsurgency (Purdue University 2001). From the perspective of those involved in force planning, the anticipated future is not one of vulnerability but unassailability.

### 2AC --- Impact

#### Any solvency deficit risks a global arms race.

Almosara 10 [Joel O.; 6/?/2010 ; The senior consultant to the Pacific Air Forces Surgeon General and commanders on occupational and environmental health programs and Deputy Director of the USAF Counterproliferation Center ; “BIOTECHNOLOGY: GENETICALLY ENGINEERED PATHOGENS,”  [https://media.defense.gov/2019/Apr/11/2002115517/-1/-1/0/53ALMOSARAMONO.PDF](file:///Users/Jayden/Library/Containers/com.microsoft.Word/Data/Library/Preferences/AutoRecovery/%20https:/media.defense.gov/2019/Apr/11/2002115517/-1/-1/0/53ALMOSARAMONO.PDF)]

The developmental trends in biological sciences indicate there is a plethora of possibilities concerning the study of microorganisms and its applicability in creating the next biological warfare agent. Both historical and recent events show the potentially devastating effect of using biological warfare agents and the terror they cause among the populace. Even more alarming is that technological advancements in the field of biological sciences will transform biological warfare agents into a new classification of genetically engineered pathogens eliciting catastrophic consequences. 2 Just as the twentieth century was the “century of chemistry and physics,” the twenty-first century will emerge as the “century of biology.” Nations, groups, and individuals that have the resources, capabilities, and knowledge to develop this technology in the year 2035 will have the global arms race advantage.

### 2AC --- Too Expensive

#### Funding extremely high totaling over 40 billion

BioSpace 22 [BioSpace Editorial Staff 9/21/2020 ; The Home of the Life Sciences Industry. Find biotech, clinical research and pharmaceutical jobs from thousands of employers; “Investment in Biopharma is Reaching an Inflection Point,” https://www.biospace.com/article/investment-in-biopharma-is-reaching-an-inflection-point-/]

Emerging biopharma companies are vital to the creation of many novel therapies and health technologies, and play an important role in the future of early-stage drug development. Little wonder U.S.-based biotech companies are the darling of private equity, venture capital companies and institutional money managers.

During the past two years, fundraising and investment in biotechnology have reached record levels. These factors have translated into elevated IPO activity and an overarching positive outlook.

Private investments have been led by healthtech and biopharma, and the first half of 2020 saw a general year-over-year increase in biotech investment. The surge was led by 26 financings of $100 million plus, totaling more than $5 billion. The first quarter of 2021, on the other hand, climbed to a record $23.4 billion in private investments, beating out the quarterly record set in Q3 2020 by 56%. This momentum continued into the second quarter of 2021 with total investment in healthtech and biopharma equalling $23.9 billion.

According to data from IQVIA, around 80% of the industry's drug development pipeline comes from emerging biopharma companies, which means small companies are the most influential in developing innovative new therapies. Emerging biopharma companies account for 84% of worldwide early-stage R&D and 73% of late-stage research.

In 2020, VC activity in biotech grew by 45%, bringing the global total to $36.6 billion USD, and the U.S. led the way.

### 2AC --- Rogue States

#### **Rogue states will use biotech to create super-soldiers.**

Malet ’11/15 [David; 11/13/15; Qualifications; "Captain America in International Relations: the Biotech Revolution in Military Affairs," <https://www-tandfonline-com.proxy.lib.umich.edu/doi/pdf/10.1080/14702436.2015.1113665?needAccess=true>, IC]

Biological weapons are typically associated with rogue states and terrorist groups; germ weapons used by weak actors against the strong. This article makes a contrary argument, that the emerging use of biotechnology by the United States, China, and other hegemonic powers is likely to afford them a new Revolution in Military Affairs (RMA), one at least as significant as the introduction of the information technology RMA that gave the United States a dominant edge over potential adversaries at the end of the Cold War. It examines recent developments and current R&D programs that call into question the rights of enemy combatants, civilian populations in target areas, and soldiers who will be physically augmented to pursue battlefield objectives. Examples include the Quikclot used to reduce fatalities in the Iraq War, which arguably prolonged public support for the war, and the Pentagon’s publicly detailed research across various programs to create super-soldiers akin to super-heroes. The real advances in biotech will likely only further retrench the major powers of the international system by conferring an asymmetric advantage far beyond the capacity of weaker actors to match.

## 5-G

### 2AC --- CP fails

#### 5G infighting causes economic nosedive – governmental disputes wreck solvency – only the plan solves

**Grossmann 22** [J. DAVID GROSSMAN, VP OF REGULATORY AFFAIRS, CONSUMER TECHNOLOGY ASSOCIATION (CTA)"US 5G leadership depends on ending government infighting," Light Reading, https://www.lightreading.com/regulatorypolitics/us-5g-leadership-depends-on-ending-government-infighting/a/d-id/776413] Blitz

From Wi-Fi and smartphones to telehealth, fitness wearables and more – wireless connectivity is a critical part of our daily lives. However, recent government infighting over spectrum use threatens the technology that so many Americans depend on. As the demand for faster and more reliable wireless connectivity continues to grow, it is time to reform our nation's spectrum policy to make sure that spectrum continues to benefit Americans. (See [After spending $117B, US carriers ask for even more 5G spectrum](https://www.lightreading.com/5g/after-spending-$117b-us-carriers-ask-for-even-more-5g-spectrum/d/d-id/776097)). Spectrum drives a large portion of consumer connectivity and technology and influences America's economy. A recent [Consumer Technology Association (CTA) study](https://cta.tech/Resources/Newsroom/Media-Releases/2022/January/Unlicensed-Spectrum-Generates-95-Billion-Per-Year) found that unlicensed spectrum generates $95.8 billion per year in incremental sales value, and there are billions more in economic benefits from licensed spectrum used by our nation's wireless providers. **DOT and FCC debris** Good spectrum policy can create jobs, spur innovation and grow GDP. Bad spectrum policy places US companies, federal agencies and American consumers at a disadvantage in a world where every country is competing to offer better technology and services. The US is risking the latter due to a lack of coordination between government agencies. For example, the recent auction of the C-band for 5G, which raised nearly $81 billion in revenue, was followed by objections from the Federal Aviation Administration (FAA). This is not the first time in recent memory that spectrum battles have erupted. There is an ongoing dispute over the repurposing of spectrum in the 5.9 GHz band between the Department of Transportation (DOT) and the Federal Communications Commission (FCC). Many more examples of bureaucratic infighting and dysfunction have littered the spectrum landscape. Sadly, these disputes are not just Beltway parlor games; they have real consequences for America's economy. American technology companies face an uncertain environment due to whether the federal government's decisions will be implemented. How can we ask companies to invest billions of dollars in a technology direction when the regulatory rug may be pulled out from under them at the last moment?

## Hybrid War

### 2AC --- Perm do both

#### Perm do both- Cooperating with EU and NATO against Russian Hybrid War tactics solves best.

**Clark 20** [Mason Clark, the Russia Team Lead and Research Analyst on the Russia and Ukraine portfolio at the Institute for the Study of War. His work focuses on Russian military adaptation and learning in Syria. His work has been cited by Task & Purpose, Defense One, the Kyiv Post, the New York Times, BBC, and others. He has briefed multiple senior military and civilian decision makers on Russian military development and the Kremlin’s global campaigns, September 2020, Institute For The Study of War, “Russian Hybrid Warfare Military Learning And The Future of War Series”, <http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf>, Pgs 9-10, JMH]

The United States should take several actions to support this revision of its strategy and approach to Russia.

• Analyze the Kremlin’s decisions within the Russian framework of hybrid war to understand and mitigate Russian lines of effort. Obfuscating the nature and purpose of Kremlin activities is a key objective of hybrid war, and US confusion about the term and the Russian approach to such conflicts hinders the development of effective counterstrategies.

• Confront Russian hybrid wars in their entirety as synthetic threats instead of confronting individual Russian lines of effort separately and partially.

• Counter the Kremlin globally as well as in Europe. Putin is not playing three-dimensional chess, but instead playing many games of checkers simultaneously. The US policy and military community should increase its analysis of the Kremlin’s hybrid wars outside Europe, including in Syria, Libya, and Venezuela while retaining necessary focus on Ukraine, Belarus, and the Baltic States.

• Pursue whole-of-government coordination of information and kinetic operations.

• Reinforce Western norms and institutions—key targets of Russian hybrid wars. The United States should not allow the Kremlin to normalize its malign behavior and worldview.

• Work to align the Russia policy of the United States and its allies. **The United States should particularly seek to standardize across NATO the red lines that would lead to responses to Russian actions.**

• Actively challenge Russian information campaigns. The Kremlin’s information campaign is its center of gravity in each hybrid war. The United States cannot win hybrid wars with Russia if it loses in the information space.

• Deprive Russian PMCs and proxy forces of their deniability. The United States and its allies must relentlessly work to expose the connections between these forces and the Kremlin and highlight that they are direct tools of Russian military policy to reduce the Kremlin’s freedom of action.

• Recognize and plan for the military requirements to confront hybrid threats. The United States should be prepared to confront Russian hybrid wars with the conventional forces that will be required and avoid establishing false red lines for the use of Western forces against Russian aggressions.

• **Recognize that Russia also aims to avoid major great power war. The US must of course continue to deter both nuclear and full-scale conventional war with Russi**a. But it must revise its strategy to recognize that Russia also seeks to avoid such conflicts while nevertheless accomplishing it goals.

• Shift its military posture to confront the global nature of the Kremlin threat.

• Enable deployed US forces to combat Russian hybrid wars with non-kinetic means. Conventional forces can act as a platform for additional cyber, civil-military relations, intelligence, technical, and special operations assets which are essential in hybrid wars.

The challenges presented by Russian hybrid war and preparations for the future of war are not insurmountable. **The West must not throw up its hands at the challenge of confronting an unfamiliar conception of the future of war. The Kremlin is optimizing for its expectations of the future of war, not ours, and the West must fully understand the Russian threat to successfully confront the Kremlin.**

## Norms

### 2AC --- CP fails

#### Norms-based approach leaves no one accountable – it is ambiguous and lacks enforcement.

MaČÁK 17[Kubo MaČÁK, Dr Kubo Mačák is a legal adviser at the International Committee of the Red Cross (ICRC). Prior to joining the ICRC in 2019, he worked as an Associate Professor of Public International Law at the University of Exeter in the United Kingdom. "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers," Cambridge University press, https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5] Blitz

While the first two indicators relate to states’ reluctance to act in ways meaningful for the generation of new rules, the third concerns their actual conduct in relation to cyber governance. It would be inaccurate to claim that states have entirely given up on standard-setting. However, instead of interpreting or developing rules of international law, state representatives have generally sought refuge in the more ambiguous term ‘norms’. It is true that law and norms are ‘intimately intertwined’ concepts and that inter-state agreement on ‘norms’ may gradually influence the development of the law.[38](https://www-cambridge-org.proxy.lib.umich.edu/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5#fn38) Yet, a fundamental difference between the two is that a violation of a binding rule of international law gives rise to international legal responsibility. while the same cannot be said of non-legal norms regulating cyber conduct.

## Space

### 2AC --- China

#### US SpaceX operations would anger China

Jim Pollard, 5-10-2022, "China Fears US Will Use SpaceX to Bring Calamity to World," Asia Financial, <https://www.asiafinancial.com/china-fears-us-will-use-spacex-to-bring-calamity-to-world>

The Starlink internet service run by Elon Musk’s SpaceX may be used by the “hegemony-obsessed US” to dominate space and bring “chaos or calamity” to the world.

That’s according to a recent commentary published by China Military Online, an official website linked to China’s Central Military Commission, which is headed by President Xi Jinping.

It expressed alarm about the use of the Starlink service in Ukraine to interact with drones, and suggested that it may have already played a role in the conflict with Russia via big data and facial recognition technology.

Also on AF: China Already Outflanks US in AI, Says Ex-Pentagon Tech Chief

“SpaceX has decided to increase the number of Starlink satellites from 12,000 to 42,000 – the programme’s unchecked expansion and the company’s ambition to use it for military purposes should put the international community on high alert,” it said. “Clearly, the military applications of the Starlink program will give the US military a head-start on the future battlefield and become an `accomplice’ for the US to continue to dominate the space.”

The report said SpaceX launched 53 satellites last month and now has 2,400 satellites in a low-earth orbit.

Strong US Military Links

While Starlink claims to be a civilian program that provides high-speed Internet services, the commentary claimed it has a strong military background, citing launch sites built within the Vandenberg Air Force Base. The group has launched satellites from American airbases and cooperated with the military “many times,” it said.

Infographic on the commentary published by China Military Online regarding The Starlink internet service run by SpaceX

Three years ago SpaceX received funds from the US Air Force to test how well Starlink satellites can relay encrypted communication to military aircraft, it said.

In 2020, the US Army allegedly signed a deal to use Starlink’s broadband to transmit data, plus a $150-million contract to develop military satellites, and last year it was transmitting data to F-35A fighter jets at speeds “30 times faster than traditional connections,” the commentary added.

Starlink’s satellites could have reconnaissance, navigation and meteorological devices added to them to enhance the US military’s combat capability to boost remote sensing, communications, navigation and positioning, attack and collision, and space sheltering, the report said.

Impressed Pentagon

Pentagon officials were impressed last month by SpaceX’s swift efforts to block an electro-magnetic attack by Russia that aimed to jam its Starlink broadband satellite service and help people in Ukraine retain their link to the internet, according to a report by Defense News.

Elon Musk allegedly boasted that “Starlink was the only non-Russian communications system still working in some parts of Ukraine in the wake of the invasion.”

There have also been reports of Starlink aiding the Ukrainian military in precision strikes on Russian tanks and forces because its high data rates enable better links. Drones could also serve as relay units to transmit data.

China’s Starlink Concerns

The China Military Online report says Starlink is already a “space juggernaut” and a megaproject that could transform global communications and give birth to “a gigantic Starlink biosphere, and monopolize the future space application market.”

It cited experts who say that if SpaceX installs a few root servers in the space, “it can make Starlink the second independent global Internet, which will pose a serious challenge to all countries in defending their cyberspace sovereignty and protecting their information security.”

#### China and US won’t cooperate now – further tensions provide an opportunity for escalation

Bin Li, 5-9-2022, "Space Won’t Be Safe until the U.S. and China Can Cooperate," Scientific American, https://www.scientificamerican.com/article/space-wont-be-safe-until-the-u-s-and-china-can-cooperate1/

China is undeniably one of the world’s top players in space these days, with successful missions to the moon and Mars and a solar probe due to be launched soon. Its rise has spurred competition with the U.S.; “Watch the Chinese,” NASA Administrator Bill Nelson recently warned. Given the strategic value the two nations have placed on their space programs, and the political tension that already exists between the countries, the contest over achievements in space is likely to intensify.

Despite the tension, the U.S. and China must figure out a way to cooperate on some, if not all, issues in the use of space. The most critical area is the safety of space infrastructure, where a lack of communication could be damaging and possibly even deadly. This need was highlighted by the recent saga of a near miss between two of Elon Musk’s Starlink satellites and China’s in-progress crewed space station. Although the Starlink spacecraft are privately owned, the U.S. government is internationally responsible for their space activities under the 1967 Outer Space Treaty.

Yet, there are serious barriers to a tête-à-tête—including the fact that some kinds of cooperation are illegal. The Wolf Amendment prohibits NASA from using government funds to engage with the Chinese government and China-affiliated organizations. However, this legislation does not block all cooperative possibilities, such as exchanging orbit information about human-made space objects through agencies like the North American Aerospace Defense Command. In the case of the Starlink satellites, U.S. representatives said they had determined that the spacecraft posed no risk to the Chinese space station. China, however, disagreed, and adjusted the station’s orbit to be safe. Cases like this could be better handled in the future through direct communication.

Both nations will continue to rely on space infrastructure for civil, commercial and national security purposes. The U.S. has 2,944 satellites, more than half of the total number of operating satellites in the world. This means that it has the most to lose from satellite collisions and risks posed by space debris. China also has a large collection, along with plans to send significant numbers of satellites to low-Earth orbit in the next few years. The risks are growing from what the U.N. calls “congested, contested and competitive” space, and it suits both countries’ interests to undertake constructive dialogues on how to keep orbital passages safe.

But the path ahead may not be smooth. The U.S. has accused China of worsening the issue, notably during a 2007 Chinese antisatellite test that created more than 150,000 pieces of space debris. Because everything in orbit is moving so fast, a collision between a small bit of debris and a spacecraft could prove catastrophic. Yet, one year later, the U.S. shot down its own satellite, although this event created fewer and shorter-lived pieces of debris, because the intercept occurred at lower altitude so the pieces burned up more quickly in Earth’s atmosphere.

Despite the acrimony, the two sides appear to agree on some important legal rules applicable to space. For instance, in a recent white paper, China professes to use outer space “for peaceful purposes.” Although this claim is open to interpretation, similar language is also widely used in U.S. space policy documents and even the Space Force’s 2020 doctrine. The fact that there is some ambiguity to the term may be a good starting point for the two countries to embark on a dialogue about whether antisatellite testing, for instance, is a peaceful activity. Although defensive in nature and not an act of war, it can pose threats to others by creating more space debris.

China appears keen to be involved in the international rulemaking process for space under the framework of the United Nations, according to statements in the recent white paper. Realistically, China can achieve this goal only through open and constructive engagement with other stakeholder nations. Promisingly, in February, when asked about the danger posed by the Starlink satellites to the Chinese space station, a Chinese spokesperson expressed willingness to establish a long-term communication mechanism with the U.S. to protect the safety of its astronauts and space station.

But the continuing finger-pointing could hold both countries back. For instance, the U.S. and China recently exchanged diplomatic fire over a U.S. unilateral commitment to stop all antisatellite missile testing. Though the move could seriously reduce the future creation of space debris, the U.S. only did so while blaming Russia and China for their previous tests. Not surprisingly, in response China demanded that the U.S. “fully reflect upon its negative moves in the field of outer space.”

To make real progress, the two countries should adopt a “think big, start small” approach. Because there is a lack of mutual trust between the two sides at this stage, it would be unrealistic to expect an agreement on space safety issues as a whole. By tackling smaller problems, such as rules about communicating when a crewed space station is at risk of collision, the two sides may more easily find common interests and are more likely to work in a cooperative manner. Thus, they can establish mutual trust in this process and, over time, expand their cooperation to other spheres in space.