Global Geo-Political Crisis: Emerging Technologies

A Topic Proposal for the
National Federation of High Schools Topic Selection Committee

Submitted

May 12, 2021

Updated

June 24, 2021

Luke Brinker-Lev
Tel-Aviv, Former Debater, Topeka HS, KS

Peter Crevoiserat
Wichita Northwest HS, KS

Michael Harris
Wichita Southeast HS, KS

Pam McComas
Retired, Director of Forensics, Topeka HS, KS

Table of Contents

Global Geo-Political Crisis: Emerging Technologies

"Never let a good crisis go to waste!"-- Sir Winston Churchill
"Crisis and opportunity"
President Joseph R. Biden, Jr.
100 Day Address, April 28, 2021

I. Introduction

As the world awaits Daniel Craig's next and final film as 007 (***No Time to Die***), everyone is excited for the next crisis facing this enigmatic character and Q's new gadgets to be unveiled to determine the best opportunity to de-escalate the situation(s). Throughout Ian Fleming's long time Bond series of fictional thrillers and espionage, the author would immerse the reader into a sci-fi glimpse of new tech for the main character to utilize in overcoming numerous threats to the United Kingdom or the world.

However, today's world is facing a global geo-political crisis with emerging technologies. Technologies, such as artificial intelligence, biotechnology, and cybersecurity are not fiction, but real and impose perilous situations to all nations. Just like Bond facing endless conflicts, in President Biden's 100-day speech, he speaks about "crisis and opportunity" ("*Biden's Speech to Congress: Full Transcript,*" ***The New York Times.com)***. Bond and Biden are of the same mindset: "turning peril into possibility, crisis into opportunity, setbacks to strength" ("*Biden's Speech to Congress: Full Transcript,*" ***The New York Times.com).*** Foremost among the crises confronting the U.S. and the world is the threat posed to liberal democracy by disinformation, attempts to dismantle core institutions, and social conflict -- phenomena that have been exacerbated by the weaponization of emerging technologies. As Rachel Ellehuus and Pierre Morcos of the Center for Strategic and International

Studies argue, now is the time for NATO to be "ambitious" in meeting this challenge and to serve as a bulwark for democratic values.

> **Ellehuus,** Rachel (Deputy Director, Europe, Russia, and Eurasia Program) **and Morcos**, Pierre (Visiting Fellow, Europe, Russia, and Eurasia Program), "'Lifting Up Our Values at Home': How to Revitalize NATO's Political Cohesion," *Center for Strategic and International Studies*, **March 12, 2021,** accessed online June 18, 2021. https://www.csis.org/analysis/lifting-our-values-home-how-revitalize-natos-political-cohesion
>
> First, an inattention to the principles of democracy, individual liberty, and the rule of law in a member country creates societal vulnerabilities that competitors can exploit. Russia, for example, preys on the grievances of racial and ethnic minorities in NATO member countries in order to weaken national-level governance and cohesion. Likewise, a compromised media environment allows disinformation campaigns to flourish, while corruption opens space for Russian networks to operate and gain influence. Even allies with strong democratic institutions, such as Germany, are increasingly targets of Russian disinformation campaigns. In these ways, a deficit in internal values quickly becomes an external security threat.

....

> Yet however difficult, NATO can no longer afford to turn a blind eye on these internal strains. From its founding, it has been more than just a military alliance. NATO has embraced a political role built on a shared democratic identity. As the alliance seeks to exercise more fully the power of this political dimension, shoring up its values is vital to realizing the full benefits of collective security. A lack of response from NATO on these issues would ultimately undermine its reputation and credibility, most notably toward accession candidates and partners.
>
> With NATO in the midst of an adaptation process and a new U.S. administration committed to defending democratic values and restoring the transatlantic alliance, the time is right for tackling this issue. Washington has the political sway to act as a "first among equals" within NATO and push allies to seriously address this challenge. However, a mere declaration of good intentions is not enough. If allies want to uplift NATO's political cohesion, they will need to be ambitious.

As James Bond would often partner with Felix Leiter, CIA operative, to conquer these challenges, the U.S. must now have a global partnership to successfully overcome various threat levels to resolve crises. This is why the authors contend a U.S. and NATO cooperative offers the best geopolitical defense against formidable threats, such as China and Russia.

Clearly, the last four years created a geopolitical climate that makes cooperation a more cumbersome sell for Biden. But, with Trump's eye on 2024, now may be the time for Biden to act decisively to partner with international groups as a way of proving their legitimacy, thus making the case for international engagement rather than isolationism. While current terrorist threats appear from domestic origins and gun violence, AI, biotechnology, and cybersecurity may pose a more dangerous threat to the United States and its allies which requires an international solution.

With experts predicting that whichever country leads in emerging technology by 2030 will be the dominant power for the remainder of this century, the time to counter the threat posed by authoritarian powers like China and Russia is running short.

> **Gill**, Indermit (Nonresident Senior Fellow, Global Economy and Development, Brookings Institution), "Whoever leads in artificial intelligence in 2030 will rule the world until 2100," *The Brookings Institution*, January 17, **2020**, online accessed 06/08/2021, https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/
>
> **A couple of years ago, Vladimir Putin warned Russians that the country that led in technologies using artificial intelligence will dominate the globe**. He was right to be worried. Russia is now a minor player, and the race seems now to be mainly between the United States and China. But don't count out the European Union just yet; the EU is still a fifth of the world economy, and it has underappreciated strengths. **Technological leadership will require big digital investments, rapid business process innovation, and efficient tax and transfer systems. China appears to have the edge in the first, the U.S. in the second, and Western Europe in the third. One out of three won't do, and even two out three will not be enough; whoever does all three best will dominate the rest.**
>
> **We are on the cusp of colossal changes. But you don't have to take Mr. Putin's word for it, nor mine. This is what Erik Brynjolfsson, director of the MIT Initiative on the Digital Economy and a serious student of the effects of digital technologies, says:**
>
> **"This is a moment of choice and opportunity. It could be the best 10 years ahead of us that we have ever had in human history or one of the worst, because we have more power than we have ever had before."**

Why should the U.S. partner with NATO? As Brynjolfsson notes, this is indeed "a moment of choice and opportunity," and given that the 2020s will be decisive in determining

which global powers lead the world in emerging technologies for foreseeable future, now is the time -- with a sufficient but rapidly shrinking window of opportunity -- to debate NATO as the appropriate mechanism for cementing the transatlantic alliance's technological and geopolitical leadership, lest China and Russia gain supremacy. Just like the CIA, NATO is in a unique position to create an innovation pipeline to maintain security worldwide. Rob Murray, the head of NATO innovation unit, contends in the ***NATO Review***, September 1, 2020, NATO is key in building the framework for emerging technology.

> **Murray**, Rob (head of the Innovation Unit, NATO's Emerging Security Challenges Division). "Building a Resilient Innovation Pipeline for the Alliance." ***NATO Review***, 1 Sept. 2020, accessed online, February 15, 2021. www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/index.html .
>
> Today, **NATO's competition is a global one and the race is one of technological adoption – that is, the acceptance, integration and use of new technology in society. From artificial intelligence to quantum and everything in between, governments are in a race to leverage these technologies at scale and speed** – **the first adopter advantage for emerging disruptive tech could not be more prevalent in the world of geopolitics and deterrence. Indeed, the nations that win this race may be those with the most agile bureaucracy rather those with the best technology.**
> **In contrast to the Cold War, the United States and its NATO Allies are unlikely to simply outspend others.** In a post-Covid-19 world, rebalancing public finances could see further financial pressure placed on Allied defence budgets. We now need a different advantage, one which will deliver in the short term and build resilience over the longer term – more defence at less cost with least delay. This starts with our people, their creativity, education and access to funding. It ends with a robust pipeline of new dual-use (civil and military) technologies constantly being created, commercialised and capitalised upon.
> **The Alliance's transatlantic nature places it in a unique position within the international order to provide both demand-side policies and supply-side resources that can genuinely build such a pipeline, creating not only innovations but entirely new markets –** as Eisenhower noted: the foundation of military strength is economic strength. Recent history would suggest, the model of democracy and Allied governments' willingness to make **big bets on mission-oriented technology** does indeed create new markets and it is this model, underpinned by shared values, which will be key to NATO's longer term success.
>
> But what about now? In the short term, **NATO innovation needs to lay the foundations for Allies to realize those benefits of an Alliance-wide approach. Answers may lay in focusing on two core areas: [1] addressing the fragmentation of researchers, academia, start-ups and government at the beginning of this pipeline – that is, managing uncertainty. [2] being able to adopt and scale these new technologies as and when they are ready – meaning the necessity of nimble, agile**

> **investment and acquisition entities across both public and private sectors, all of which need to be equally incentivized to take significant levels of risk.**
> **These activities are difficult in their own right but combining them into an Alliance innovation pipeline,** while attempting to make use of the comparative advantage each Ally brings to the table, leaves the Alliance with a "wicked problem". It is wicked because it **demands a combination of both sustained and disruptive innovation (which seeks to radically change the status-quo) occurring simultaneously across NATO.**

In addition, European leaders now view this as a critical time to develop the types of alliances that were not possible under the previous administration:

> **Erlanger,** Steven (chief diplomatic correspondent) **and** Michael D. **Shear** (White House correspondent), "Shifting Focus, NATO Views China as a Global Security Challenge," *The New York Times*, **June 14, 2021**, accessed online June 24, 2021, https://www.nytimes.com/2021/06/14/world/europe/biden-nato-china-russia.html
>
> **New challenges from cyberwarfare, artificial intelligence and disinformation, as well as new missile and warhead technologies, must be considered to preserve deterrence, the alliance said. And Article 5 of its founding treaty — an attack on one is an attack on all — will be "clarified" to include threats to satellites in space and coordinated cyberattacks.**
>
> **This NATO meeting was mostly a warm embrace of President Biden, who in contrast to his predecessor has expressed deep belief in the alliance and in the importance of American participation in the multilateral institutions Washington established after the horrors of World War II.**
> **The contrast to Mr. Trump's May 2017 NATO summit was remarked on by many other leaders.** Then, Mr. Trump was particularly angered by the expense and lavish use of glass in NATO's new $1.2 billion headquarters. Mr. Trump also defied the expectations of even his own aides and refused to announce support for NATO's Article 5, a central tenet of collective defense.
>
> **Mr. Biden quickly declared Monday that the alliance is "critically important for U.S. interests" and called Article 5 a "sacred obligation." He added: "I just want all of Europe to know that the United States is there."**
>
> **Prime Minister Mario Draghi of Italy spoke for many when he connected this summit with the Group of 7 summit meeting just concluded in Britain and compared them unfavorably with the period of Mr. Trump. "This summit is part of the process of reaffirming, rebuilding the fundamental alliances of the United States," which were "weakened by the previous administration," Mr. Draghi said.**

With a new administration taking the reins, now could be the key opportunity of moving forward with international partnerships, particularly in the area of emerging technologies. On February, 2021, at the Munich Security Conference, President Biden argues,

> We must shape the rules that will govern the advance of technology and the norms of behavior in cyberspace, artificial intelligence, biotechnology so that they are used to lift people up, not used to pin them down. We must stand up for the democratic values that make it possible for us to accomplish any of this, pushing back against those who would monopolize and normalize repression.

In a recent ***Brookings Institute*** report, Lindsey Ford, a David M. Rubenstein Fellow, and James Goldgeier, a Senior Visiting Fellow in Foreign Policy, contend,

> **Ford**, Lindsey W**. (**David M. Rubenstein Fellow-Foreign Policy, Ctr. For East Asia Policy Studies) **and** James **Goldgeier (**Sr. Visiting Fellow-Foreign Policy, Ctr on US and Europe)**, "**Retooling America's Alliances to Manage the China Challenge." ***The Brookings Institute,*** **Jan. 25, 2021, online accessed 02/15/2021,** https://www.brookings.edu/research/retooling-americas-alliances-to-manage-the-china-challenge/
>
> **The first step in creating more capable 21st century alliances is to return to basics: focusing on the defense of allied sovereignty**. While allies can and should play important roles addressing violent extremism in the Middle East or engaging in partner capacity-building efforts in Africa, **the principal focus of U.S. alliances in Europe and Asia should be to maintain a credible deterrence and self-defense capability. This will require greater investments by U.S. allies in their own defense, but it will also require a greater willingness in Washington to allow allies to take the lead in their own regions. Despite Europe's continued dependence on the United States, it is time for a reconceptualization of the trans-Atlantic relationship**. NATO's continuation after the end of the Cold War was a way of keeping America in charge of European security during an uncertain period after the Soviet collapse. Europe's failure to stop genocide in the former Yugoslavia in the early 1990s was another reminder of the continent's dependence on Washington, which finally put an end to the killings. **Moving forward, NATO's success should be measured by its ability to shift from serving as a vehicle for U.S. dominance over European security to an entity that enables the U.S. to assist European-led defense efforts in a more balanced partnership**.
>
> **In October 2020**, **German Minister of Defense Annegret Kramp-Karrenbauer** spoke of Germany's continued dependence on the U.S. for nuclear deterrence, but declared that her country's defense budget would continue to rise despite pressures caused by the pandemic. She **argued it was time for Germany, and Europe, to do more: "We Europeans will have to do ourselves much of what America has largely done for us so far, by diplomatic and by conventional military means. Securing NATO's eastern flank. Crisis management operations in our immediate neighborhood outside of Europe. Air and**

sea surveillance… We stay dependent, but at the same time, we must come into our own."

If the U.S. is going to succeed in rebalancing its defense posture toward Asia, it needs a stronger Europe able to take the lead in its broader neighborhood. Fears that European efforts to build greater capacity will undermine NATO are overblown and only relevant in a world in which U.S. dominance over European security — rather than the capacity of European allies to manage their own security challenges with less reliance on the United States — is the primary goal.

The U.S. needs to continue encouraging its allies to move out of a supporting role in the Indo-Pacific as well. In light of the rapidly advancing military threat from both China and North Korea, U.S. allies will need to play a larger role in not only their own self-defense, but also in the region. An increasing tempo of allied air and maritime presence operations will be particularly valuable in the coming decade as the United States looks to address needed modernization requirements that may reduce its bandwidth for steady state operations. If the U.S. wants to "shift" the defense burden and credibly deter Beijing, it should also explore new ways to make it easier for U.S. allies to obtain the capabilities they need. This should include breaking down outdated bureaucratic hurdles, export control rules, and technology transfer restrictions that can make it difficult for U.S. allies to compete more effectively with Beijing. Equally important, many of these restrictions often incentivize U.S. allies to pursue autonomous capabilities outside of the alliance, rather than in tandem with Washington.

Finally, focusing on domestic resilience in space, cyberspace, and technological systems will create additional incentives for allies to work together. The threat China poses in these arenas as it seeks to take the lead in 5G and artificial intelligence (AI) is becoming more apparent to allies in Asia and Europe: this is one area that can foster greater consensus despite allied disagreement on the political and economic challenges that Beijing poses.

To be sure, NATO has already signaled its willingness to act on the threat posed by emerging technology. At the alliance's June 2021 summit, member states agreed to launch a defense innovation accelerator and to increase NATO's advisory role on cybersecurity.

Tucker, Patrick (technology editor), "NATO Members Agree to Broad Tech Agenda, Environmental Agenda," *Defense One*, **June 16, 2021**, accessed online June 18, 2021. https://www.defenseone.com/threats/2021/06/nato-members-agree-broad-tech-agenda-environmental-agenda/174767/

NATO members will determine the best way to identify and minimize cyber threats, as they always have, but the members agreed to a more active advisory role for NATO. They also agreed to start the process of sharing more information with each other about the status of their resilience efforts.

"There is a political commitment to develop this whole process, so to create...a system for monitoring, to come together regularly with high-level officials from all countries to monitor progress and then, of course, on the basis of these objectives…each ally will work with us advising to develop their own national approach. It's an expansion."

NATO members will launch a defense innovation accelerator to help fund startups develop technology that could help collective defense.

"Concretely, this will be a center designed to foster greater transatlantic cooperation, to promote interoperability and that will have a series of...offices to staff centers across the alliance," she said. The accelerator will allow NATO to better "experiment, validate, integrate, [and] adopt new and emerging technologies, together."

Members have also agreed to launch a defense innovation fund focused on startups that make technology for both defense and civilian organizations. The fund will be opt-in and will look for new, non-traditional players making technologies "that answer problems we have for our common defense and security," Berti said, describing it as a recognition that the next generation of companies making defense products will largely be software companies.

But, while NATO's pledges to increase technology cooperation are a step in the right direction, defense scholars including Jamie Shea and Michael John Williams contend that this is just the beginning, and in "a world full of competition for attention," more will need to be done to confront the emerging technology crisis head-on.

Shea, Jamie (president at the Centre for War Studies at the University of Southern Denmark and a former NATO deputy assistant secretary general for emerging security challenges) **and Williams**, Michael John (nonresident senior fellow with the Scowcroft Center's Transatlantic Security Initiative and an associate professor of international affairs at Syracuse University), "The secret to NATO's survival: Get political," *Atlantic Council*, **June 17, 2021**, accessed online June 18, 2021. https://www.atlanticcouncil.org/blogs/new-atlanticist/the-secret-to-natos-survival-get-political/

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

> **Developing the Alliance as a political actor via these six action points will not be easy, but if there is an administration that could do it, it is Joe Biden's. Biden is the first US president since George H.W. Bush with an inherent tendency toward Atlanticism.** Since 2000, the transatlantic space has endured reproach, apathy, and most recently hostility and neglect from the White House, all of which have been highly detrimental to transatlantic relations and greatly contributed to the decline of NATO as a political actor. But Biden is a natural trans-Atlanticist and is the last president of a generation that looked instinctively to Europe. **One of his chief legacies could be setting a foundation for younger Americans to see Europeans, in a world full of competition for attention, as the allies they turn to first.**

Artificial Intelligence (AI)

In the 65 years since computer scientist, John McCarthy, coined the term "artificial intelligence," AI has alternately captivated, enthralled, inspired, confused, terrified, and troubled scientists, philosophers, political commentators, and the public. In fact, global Bond enthusiasts are even using AI to predict the next actor to be 007.

Depending on one's vantage point, AI may represent an opportunity to either hope for a future in which human beings are liberated from mundane jobs and tasks and free to pursue their own creative and leisurely interests, or an existential threat to livelihoods and the dignity of work for all, but a narrow technocratic elite. It may be an enabler of unprecedented efficiency, or yet another tool for flattening, and thereby impoverishing the human experience. One could see AI as a promising pathway to smarter, more data-driven, less biased decision-making, or simply a hi-tech means of replicating deeply ingrained societal biases, but with even less accountability. Where some see a resource for building smarter cities and safer streets, others fear that AI will serve as a weapon for making the modern surveillance state even more intrusive. Whereas many AI enthusiasts hail the technology as a way of facilitating connections among people with shared values, interests, and ideas, more skeptical minds may consider the technology a leading culprit behind the Balkanization of 21-century social and political life. For every champion of AI as a

solution for making modern warfare more precise, with fewer civilian casualties, there are likely just as many who worry AI may be a precursor to killer robots.

Extensive as this list is, it is by no means exhaustive. AI encompasses a broad range of applications and use cases; indeed, it is a term that "refers to any human-like intelligence exhibited by a computer, robot, or other machine. In popular usage, artificial intelligence refers to the ability of a computer or machine to mimic the capabilities of the human mind" (IBM). AI systems rely on data inputs to generate insights that can then be wielded by human beings to make decisions. For instance, AI can be utilized to forecast electoral outcomes based on diverse inputs like social media sentiment analysis, demographic and economic conditions, polling data, and so on (Wiggers, 2020).

AI can be as simple and mundane as the auto-fill that predicts and suggests words and phrases for our text messages and email communications (usually with uncanny accuracy, based on an extensive, data-driven understanding of online communication). It can be as complicated and controversial as the algorithms that some experts suggest will help guide foreign policy decision-making in the years to come (Choi, 2019).

To the extent that AI provokes unease and debate, it is less because of what people think of AI as a "concept" and has much more to do with what people think of specific applications of the technology. And, when it comes to the role AI will play in international affairs and security, there is ample room for contention.

While AI may not be at the forefront of most international affairs discussions, it is already a prominent factor in one of the central animating realities of global geopolitics: the great power competition, verging on a global crisis, between the United States and the People's Republic of China.

For all that President Joe Biden has done to roll back key elements of former President Donald Trump's domestic and foreign policies, the 46th president and his administration have signaled that they will continue his predecessor's tough line against China (Lee, 2021). The bipartisan consensus that China is, at best, a strategic competitor stems in large part from a clear-eyed assessment of the country's vast geostrategic ambitions, which has led many to the conclusion that the U.S. was misguided in its turn-of-the-century gamble that liberalizing economic and trade relations with China would foster greater political liberalization in the country and encourage "peace and security" on the global stage (Clinton, 2000).

Evidence against former President Clinton's assessment can be found from China's actions in the South China Sea, its close ties with adversarial regimes like Iran and North Korea, and its alleged theft of intellectual property. In the realm of AI, President Xi Jinping has been clear that he sees Chinese supremacy as a core foreign policy and national security objective and has formulated a strategy for Chinese predominance in the field by 2030.

> **Allison**, Graham (Professor of Government at Harvard University's John F. Kennedy School of Government), **and** Eric **Schmidt** (Chair of the US National Security Commission on Artificial Intelligence. "Is China Beating the U.S. to AI Supremacy?" ***Harvard Kennedy School, Belfer Center for Science and International Affairs,*** August **2020**. https://www.belfercenter.org/publication/china-beating-us-ai-supremacy
>
> Kai-Fu Lee's book AI Superpowers offers an insightful summary of **China's engagement in the field**. It **began with President Xi Jinping**'s personal reaction to the defeat of the world's Go champion. **Declaring that this was a technology in which China had to lead, he set specific targets for 2020 and 2025 that put China on a path to dominance over AI technology and related applications by 2030**.12 Recognizing that this would have to be led by entrepreneurial companies rather than agencies of government, he designated five companies to become China's national champions: Baidu, Alibaba, Tencent, iFlytek and SenseTime.13 **Twelve months after Xi's directive, investments in Chinese AI startups had topped investments in American AI startups.**14 **By 2018, China filed 2.5 times more patents in AI technologies than the United States.**15 **And this year China is graduating three times as many computer scientists as the United States.**

Then, President Trump sought to assert U.S. leadership in the field with a 2019 executive order establishing the American AI initiative.

> "The National Intelligence Research and Development Strategic Plan: 2019 Update." **Select Committee of Artificial Intelligence of the National Science & Technology Council, June 2019**. https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf
>
> On **February 11, 2019, the President signed Executive Order 13859, Maintaining American Leadership in Artificial Intelligence.** 7 This order launched the American AI Initiative, a concerted effort to promote and protect AI technology and innovation in the United States. **The Initiative implements a whole-of-government strategy in collaboration and engagement with the private sector, academia, the public, and like-minded international partners.** Among other actions, **key directives in the Initiative call for Federal agencies to prioritize AI R&D investments, enhance access to high-quality cyberinfrastructure and data, ensure that the Nation leads in the development of technical standards for AI, and provide education and training opportunities to prepare the American workforce for the new era of AI.**

But, critics suggest Trump's executive order fell short of what would be needed to promote U.S. AI leadership.

> **Metz,** Cade (technology correspondent). "Trump Signs Executive Order Promoting Artificial Intelligence." ***The New York Times,*** February 11, **2019.** https://www.nytimes.com/2019/02/11/business/ai-artificial-intelligence-trump.html
>
> **President Trump signed an executive order** Monday **meant to spur the development and regulation of artificial intelligence**, technology that many experts believe will define the future of everything from consumer products to health care to warfare.
>
> **A.I. experts across industry, academia and government have long called on the Trump administration to make the development of artificial intelligence a major priority**. Last spring, worried that the United States was not keeping pace with China and other countries, Jim Mattis, then the defense secretary, sent a memo to the White House imploring the president to create a national strategy on A.I.
>
> Now, Mr. Trump has taken that step, though **this "American A.I. Initiative" might not be as bold as some had hoped.**
>
> **The executive order aimed to better educate workers in the field, improve access to the cloud computing services and data needed to build A.I. systems, and promote cooperation with foreign powers. But the order did not set aside funds for A.I. research and development, and the administration provided few details on how it planned [to] put its new policies into effect.**

The Biden administration plans to continue the previous administration's efforts to counter China's AI ambitions and may take additional steps, including on U.S. manufacturing policy, to escalate the competition.

> **Hao**, Karen (senior AI reporter at MIT Technology Review). "The Biden administration's AI plans: what we might expect." ***Technology Review,*** January 22, **2021**, https://www.technologyreview.com/2021/01/22/1016652/biden-administration-ai-plans-what-to-expect/
>
> Finally, Biden's new secretary of state made clear that technology will still be an important geopolitical force. During his Senate confirmation hearing, **Antony Blinken remarked that there is "an increasing divide between techno democracies and techno autocracies. Whether techno democracies or techno autocracies are the ones who get to define how tech is used…will go a long way toward shaping the next decades.**" As pointed out by Politico, **this most clearly is an allusion to China, and the idea that the US is in a race with the country to develop emerging technologies like AI and 5G.** OneZero's Dave Gershgorn reported in 2019 that this had become a rallying cry at the Pentagon. Speaking at an AI conference in Washington, Trump's Secretary of Defense Mark Esper, framed the technological race "in dramatic terms," wrote Gershgorn: "A future of global authoritarianism or global democracy."
>
> Blinken's comments suggest to me that **the Biden administration will likely continue this thread from the Trump administration. That means it may continue putting export controls on sensitive AI technologies and placing bans on Chinese tech giants to do business with American entities. It's possible the administration may also invest more in building up the US's high-tech manufacturing capabilities in an attempt to disentangle its AI chip supply chain from China.**

At stake in the AI competition is much more than bragging rights. Economic leadership and global security hang in the balance.

> **Levine**, Steve (Future Editor at Axios. I am a Senior Fellow at The Atlantic Council, and teach energy security at Georgetown University). "The stakes for who wins the AI race," ***Axios.*** March 21, **2018**. https://www.axios.com/the-stakes-for-who-wins-the-ai-race-0363d9cd-0d97-4a5a-9ee6-36a7fb03ff44.html
>
> Robert Work, a former deputy secretary of defense in the Obama Administration, tells Axios that that dichotomy — the difference between democratic and authoritarian systems — mean that "how we use AI will be different."
> **In September,** for instance, **Vladimir Putin said that whoever leads AI "will become the ruler of the world." Given Putin's effort to "attack the cohesion of democratic countries" the last two years, if he did have sophisticated AI, he "would be able to probe divisions of the entire society," Work said. "Russia looks at this as 'active**

measures,'" meaning as part of its longstanding system of clandestine attack on other countries.
Russia is behind in AI research but ahead on robotic warfare, said Work, who is a board member at Govini, an analytics firm.
With China, the AI race is likelier to have an economic texture, said Andrew Moore, dean of computer science at Carnegie Mellon University. "It will be the economic question of who will be the Googles, Amazons and Apples in 2030. There is a good chance they are more likely to come out of China than the U.S.," Moore tells Axios.

The main reason is human capital: Moore estimates that China produces ten times the number of university graduates specializing in AI as the U.S.

While China is the United States' primary geopolitical rival in AI, Russia has substantially increased its strategic initiatives in AI in recent years, particularly in the commercial realm.

Markotkin, Nikolai (expert with the Russian International Affairs Council), **and** Elena **Chernenko,** (journalist with Kommersant newspaper).
"Developing Artificial Intelligence in Russia: Objectives and Reality." ***Carnegie Moscow Center,*** Aug. 5, **2020**. https://carnegie.ru/commentary/82422

Russia's leaders have been paying close attention to artificial intelligence (AI) technologies for several years now. **President Vladimir Putin has said on numerous occasions that the leader in the field of AI would become "the master of the world." Until recently, however, Russia remained virtually the only large country without its own AI development strategy.**

That changed in October 2019, when the country adopted a long-discussed National Strategy for the Development of Artificial Intelligence Through 2030. One of the driving forces behind the strategy was Sberbank president German Gref. **The state-owned bank has also developed a road map for developing AI in Russia and coordinated the creation of Russia's AI development strategy, which is largely corporate**, involving the internet giants Yandex and Mail.ru Group, along with Gazprom Neft energy company.

…

Russian businesses are willing to put AI technology into practice, giving Russia a competitive advantage. **Microsoft has named Russia the world leader in the active implementation of AI in business. According to its research, 30 percent of Russian companies actively implement AI: the highest number among all countries studied, compared with an average of 22.3 percent.**

Recognizing that AI's role in international security will only grow more prominent in the coming years, NATO aims to develop a set of common AI standards by the summer of 2021. The precise

form these standards will take remains to be seen, but they may provide a useful framework for new policy development.

> **Heikkila,** Melissa (POLITICO Europe's AI Correspondent). "NATO wants to set AI standards. If only its members agreed on the basics," ***Politico*****.** Mar. 29, **2021**, https://www.politico.eu/article/nato-ai-artificial-intelligence-standards-priorities/
>
> On paper, **NATO is the ideal organization to go about setting standards for military applications of artificial intelligence**. But the widely divergent priorities and budgets of its 30 members could get in the way. **The Western military alliance has identified artificial intelligence as a key technology needed to maintain an edge over adversaries, and it wants to lead the way in establishing common ground rules for its use.**
> "**We need each other more than ever. No country alone or no continent alone can compete in this era of great power competition,"** NATO Deputy Secretary-General Mircea Geoană, the alliance's second in command, said in an interview with POLITICO. **The standard-setting effort comes as China is pressing ahead with AI applications in the military largely free of democratic oversight. David van Weel, NATO's assistant secretary general** for emerging security challenges, **said Beijing's lack of concern with the tech's ethical implications has sped along the integration of AI into the military apparatus. "I'm ... not sure that they're having the same debates on principles of responsible use or they're definitely not applying our democratic values to these technologies,"** he said. Meanwhile, the EU — which has pledged to roll out the world's first binding rules on AI in coming weeks — is seeking closer collaboration with Washington to oversee emerging technologies, including artificial intelligence. But those efforts have been slow in getting off the ground. For Geoană, that **collaboration will happen at NATO, which is working closely with the European Union as it prepares AI regulation focusing on "high risk" applications.**
>
> …
>
> **NATO does not regulate, but "once NATO sets a standard, it becomes in terms of defensive security the gold standard in that respective field,"** Geoană said. The alliance's own AI strategy, to be released before the summer, will identify ways to operate AI systems responsibly, identify military applications for the technology, and provide a "platform for allies to test their AI to see whether it's up to NATO standards," van Weel said.

Biotechnology

Biotechnology has been a part of human society for as long as documented history. Early forms of biotechnology include the use of yeast to leaven bread, as well as the use of algae to make cakes. These ancient forms of biotechnology may have been emerging technologies at one point in human history, but today, the use of biological organisms or their byproducts for mundane matters like making cheese and yogurt are not what comes to mind when the term

biotechnology is used. The term was first documented in 1919 by a Hungarian engineer, but this was not the real beginning of biotechnology's importance or development. There are clear phases of development in the science of biotechnology extending from ancient uses in agriculture, to classical developments during the 19th century, and finally extending to today's modern period of exponential development (Verma, et al, 2011). Modern biotechnology has even taken on an air of science fiction. As readers and viewers of the Bond series, Q introduces the audience to biotechnology with "smart blood" used in ***Spectre*** to track 007, which is no longer far off the mark of realized science as DNA databases grow in size and scope. Again, another opportunity for crisis facing the world.

The evolution of biotechnology toward an understanding of genes and their influence on health defines the modern iteration of biotechnology and certainly gains the most attention. In the last two decades, CRISPR technology, a relatively esoteric niche, has been widely discussed and debated. It is a gene editing tool with the potential to revolutionize the treatment of disease at the genetic level (Ledford, 2020). It also offers prospects for the development of agriculture and energy through the creation of disease resistant crops and biofuels (Weiss, 2016). However, biotechnology is not without risks. As with any technology, the potential for misuse exists. This is particularly true for technologies described as "dual-use," where the innovation can be employed to benefit or harm society. These possibilities include but are not limited to the following:

> **Galatas**, Ioannis. "The misuse and malicious uses of the new biotechnologies", Annales des Mines - Réalités industrielles, vol. février 2017, no. 1, **2017**, pp. 103-108.

- **Bio-defense**: Scientific and technological changes in detection, identification, diagnosis and protection provide increased capabilities to counter or protect against biological weapons.
- **Genetic modifications**: Considerable research on genetically modified live vaccines able to immunize simultaneously against multiple antigens while

knowledge of the molecular basis of antigens led to antibody reagents of improved specificity.

- **Mechanism of action of micro-organisms**: Using molecular biology, **mechanisms of virulence and infection have been identified, raising fears for deliberate manipulation of these mechanisms** (e.g. via transferring genetic traits into naturally infectious micro-organisms or via altering their immunogenicity thus invalidating both vaccines and diagnostic methodologies).
- **Micro-biological developments**: Better knowledge of protein synthesis and assembly led to production and isolation of various proteins (e.g. Escherichia coli; Yersinia spp.).
- **Human Genome Project (HGP)**: Identification and localization of genes causing hereditary diseases and simplification of the development of pharmaceutical drugs for treatment of hereditary diseases. **HGP provides sufficient data on ethnic genetic differences between population groups, raising fears for future "ethnic bombs" (micro-organisms attacking known receptor sites or targeting DNA sequences inside cells by viral vectors)**. A study in the US on the Y-chromosome and mitochondrial DNA in populations from different regions has suggested that the data generated could be used for developing methods to selectively disturb cellular respiration and energy exchange, sexual reproduction and a number of other important functions connected with the Y-chromosome. A recent study in Taiwan has discovered that Severe Acute Respiratory Syndrome (SARS) can be associated with specific genetic profiles. Human Genome Project (HGP) – completed in 2003 – discovered all the estimated 20,000-25,000 human genes and determined the complete sequence of the three billion DNA subunits bases in the human genome.
- **Toxins and Regulators**: Large-scale extraction and production (lower cost/shorter time) of potent toxins, which until now were available only in minute quantities from immense amounts of natural biological materials. Understanding of bio-regulators and their effects, when present in abnormal concentrations. **The possibility to manipulate toxins or bio-regulators or to produce them in pure form in large quantities opens up new perspectives that have to be considered with implications for BTWC. Bio-regulators are considered to pose a serious threat of being used for illicit purposes due to the increased understanding of inter- and intra- cellular processes and control of central biological processes of mammalian systems, including human.** Much interest these days has been generated in identification and purification of toxins from marine resources having therapeutic potential. Though isolated in small quantities, they have already been shown to have potential of exploitation for generating significant amounts of bioactive substances of both therapeutic and harmful effects. Recently a bioactive peptide, a synthetic conotoxin compound produced by cone snails, has been licensed for use in the treatment of severe chronic pain. Botulinum toxin is a therapeutic for a number of disease conditions. The catalytically active and toxic A-subunit portion of these toxins conjugated with antibodies raised against specific antigens found on the surface of tumour cells is used for site-directed anticancer therapy. B-subunit toxins are being exploited to study intracellular delivery mechanisms like delivery of therapeutic agents to neural cells for the

> treatment of neural dysfunctions. It is also well known that botulinum toxin is a potential bio-agent for military use.

Biotechnology's array of applications is apparent in healthcare, agriculture, environmental protection, and even energy. In each of these areas, potential cases could act to improve cooperation to benefit innovation or manage risk. Avenues for the employment of biotechnology seem limitless. For example, biotechnology has made it possible to create edible vaccines. Innovations of this type are exciting as they have the potential to prevent common diseases particularly in developing countries.

> **Kurup**, Vrinda M, and Jaya **Thomas**. "Edible Vaccines: Promises and Challenges." Molecular biotechnology vol. 62,2 (**2020**): 79-90. doi:10.1007/s12033-019-00222-1
>
> **Edible vaccines offer a better choice predominantly in developing countries because they are cost-effective, easily administrable, no storage issues and bio-friendly.** Edible vaccines provide mucosal activity along with systemic immunity. **Plant-based vaccines are comparatively more easier to manufacture, while normal vaccine production requires highly sophisticated and expensive techniques for bulk production as in mammalian and microbial cell culture** . The statistics show that the entire population in China requires only 40 acres of land for production of hepatitis B edible vaccines annually. As per this, 200 acres of plot is required for the production of edible vaccine for all infants in the world [15]. **Various edible products like plants, algae, insect cells, whole yeast and lactic acid bacteria are used as alternative agents for parenteral vaccines** [15].

Examples such as this, demonstrate biotechnology's broad range of utilization. The opportunities for international cooperation across a host of issues makes biotechnology a rich source of policy options for debaters.

In addition, biotechnology is a prime example of how domestic action may not go far enough to influence the path of technology innovation and use. While the U.S. may be able to control where innovation occurs for domestic entities, there is growing concern that it will not be able to exert as much influence in the future. When considering international competition, one potential risk for US security is China's aggressive development of biotechnology. While the

U.S. is still dominant in this area, indications show that China is a growing threat. Furthermore, there are mutual risks to both countries from unregulated use of biotechnology and its potential misuse by terrorist groups. This highlights China as an important adversary and counterpart in international biotechnology initiatives.

> **Moore, Scott** (Director of China Programs and Strategic Initiatives, University of Pennsylvania). "China's Role in the Global Biotechnology Sector and Implications for US Policy." **Brookings Institute**. April **2020**. https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_china_biotechnology_moore.pdf
>
> **The certainty that China will play an increasingly important role in the global biotechnology sector poses several issues for U.S. policymakers. The gravest of these pertain to national security**. Though there is presently no sign that China's capabilities exceed those of the United States, some researchers have noted that **biotechnology is a focus of increasing attention by the People's Liberation Army**. U.S. policymakers and security analysts have also raised concerns that the **dominant market position of Chinese firms in producing active pharmaceutical ingredients might allow Beijing to disrupt U.S. access to lifesaving drugs in the event of a conflict**. On the other hand, **the use of tools like CRISPR, which is increasingly inexpensive and easy to use, by terrorists and non-state actors to potentially create novel bioweapons poses severe security threats to both the United States and China. It would seem to be in the interest of all states, including China, to strengthen efforts, currently led mostly by the private sector, to prevent dangerous actors from gaining access to DNA templates and other relevant materials**

Biotechnology also converges with the other areas of the topic in important ways. This offers debaters the opportunity to address multiple concerns within a debate round. A synergy between topic areas allows affirmative teams to explore unique solvency options and advantages while providing negative teams ground to explore gaps in solvency for potential cases.

> **Richardson**, Lauren C (author) et al. "Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape." ***Frontiers in bioengineering and biotechnology*** vol. 7 99. **6 Jun. 2019**, doi:10.3389/fbioe.2019.00099
>
> **Industry interest in artificial intelligence (AI) has experienced a resurgence in recent years** due to increased computing power, advancing applications of neural networks, and an emergence of new machine and deep learning techniques across the biology sector**.** Biotechnology companies are successfully utilizing these developments for drug design and development (Zilinskas, 2017), genomics (Pauwels and Vidyarthi, 2017), evolutionary biology (Feltes et al., 2018), protein folding (Paladino et al., 2017), and more. **This rapid and evolving interest in the landscape of new AI technologies has led to emerging threat domains related to information privacy and storage, ownership over biological and genetic data, and applications of**

> **powerful technologies** (Pauwels, 2018). These issues are not new, as bioinformatics and digitization have created a potential target; however, the popularization of AI has refreshed these concerns in the modern zeitgeist. **There is a renewed opportunity for life science and cybersecurity professionals to design and implement frameworks to facilitate responsible application of AI techniques to biology.**

In conclusion, the international response to biotechnology is an important factor for debate. Can the international community afford not to act to prevent the potential harms of biotechnology? Could the international community provide meaningful guidance for biotechnology without stifling innovation? Is international cooperation key to stimulating creativity in the field of biotechnology? Will the global community be prepared to respond to biological threats both naturally occurring or man-made in the future? These questions are central to the debate over US international cooperation on emerging technologies in the field of biotechnology.

Cybersecurity

In the 2012 production of ***Skyfall***, British intelligence is facing an unknown cybersecurity threat designed to wreak havoc on M16, Bond, and the world. But, in the real world, the United States faces the biggest risk during the Trump administration, and now, the current administration, as well. Currently, the U.S. confronts a similar crisis from Russian and Chinese hackers who want to gain access to U.S. servers. Cyberspace creates a unique vulnerability for attack in the United States as laws block the ability of intelligence agencies to use domestic internet service providers as a base for attacks.

Lawmakers are being tasked, by the NSA and our nation's leading cybersecurity experts, to create solutions preventing hackers' access to U.S. servers. The recent exploitation of Microsoft Exchange servers, by the Russian and Chinese governments, left the U.S. blind to the cyber intrusion. On May 8, 2021, DarkSide (alleged Russian hackers) breached the Colonial Pipeline, part of U.S. energy infrastructure, to create chaos. Whether this is in response to

President Biden's sanctions on Russia, is unknown. However, NSA can only monitor foreign internet traffic. NSA would have to request lawmakers to expand their domestic cyber authority for limited circumstances. This is a concern for lawmakers because of watchdog and 4th Amendment privacy rights' groups, as the U.S. has a long and documented history of using broad surveillance authority to collect information about its citizens. However, a failure to take action means ceding Russian, Chinese, North Korean, Iranian, and other non-state hackers' access to critical public and private systems in the U.S. The Council of Foreign Relations counters this pressure by reminding decision makers that there is no indication that expanding the scope of NSA authority would have resulted in discovering the recent Solar Wind attacks. Tonya Riley, technology and cybersecurity researcher for the ***Washington Post***, argues:

> **Riley**, Tonya (Technology and cybersecurity policy researcher). "Analysis | The Cybersecurity 202: NSA Director Says Intelligence Has a Big Blind Spot: Domestic Internet Activity." ***The Washington Post, WP Company,*** 26 Mar. 2021, www.washingtonpost.com/politics/2021/03/26/cybersecurity-202-nsa-director-says-intelligence-has-big-blind-spot-domestic-internet-activity/#click=t.co/kg8XkfRoXH.
>
> National Security Agency Director Gen. Paul Nakasone stressed that foreign hackers are taking advantage of the intelligence community's "blind spot" – domestic Internet activity. "**Our adversaries understand that they can come into the United States and rapidly utilize an Internet service provider, come up and do their activities, and then take that down before a warrant can be issued, before we can actually have surveillance by a civilian authority here in the United States**," he told the Senate Armed Services Committee in a rare hearing. **Washington is scrambling for solutions in light of two major recent hacks in which attackers used U.S. internet infrastructure. In a sweeping Russian hack of at least nine government agencies and 100 companies, hackers used Amazon cloud services and GoDaddy domains to launch malicious software used in the attack. Those hackers went unnoticed by the government for almost nine months. Chinese hackers that compromised thousands of Microsoft Exchange servers also used U.S. based servers**. "It's not the fact that we can't connect the dots. We can't see all of the dots," Nakasone told lawmakers. **The NSA only has authorization to monitor foreign Internet traffic. And although the FBI and the Department of Homeland Security have some authority over Internet traffic within the United States, the authorities require a warrant. It's against this backdrop that some experts want to expand NSA authorities to monitor domestic Internet traffic under limited circumstances.**

Instead, the Council recommends the U.S. should focus on creating public-private partnerships (PPP's) to combine cyber intelligence and coordinate more effective responses to threats. These

PPP's do not come without their own concerns. Private industry is reluctant to share discovery of software vulnerabilities with the U.S. government and the National Security Agency (NSA). These organizations consistently refuse to fix vulnerabilities and instead engage in a policy of leaving "Backdoors" for future Offensive Cyber Operations (OCO's). Regardless of concerns, lawmakers are currently drafting legislation requiring private companies to disclose these vulnerabilities to the U.S. government and its agencies.

Analysis of the recent Solar Winds attacks by private cyber security firms carrying out the ongoing attacks on the U.S., European governments, and private businesses confirm the impact of this breach. The examination of the servers reveals the groups responsible for the attack, the scope and breadth of the attacks, and the far-reaching nature of their exploitation of a vast array of targets, Covid-19 test manufacturers, and defense and aerospace companies. Analysis of hacking patterns discloses EvilCorp as the culprit.

> **Lepido, Daniele (senior reporter for Bloomberg News).** "Swiss Cyber Security Firm Says It Accessed Servers of a SolarWinds Hacking Group." ***Insurance Journal,*** **3-23-2021,**
> https://amp-insurancejournal-com.cdn.ampproject.org/v/s/amp.insurancejournal.com/news/international/2021/03/23/606548.htm?amp_gsa=1&amp_js_v=a6&usqp=mq331AQFKAGwASA%3D -amp_tf=From%20%251%24s&aoh=16166058694112&csi=0&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fwww.insurancejournal.com%2Fnews%2Finternational%2F2021%2F03%2F23%2F606548.htm
>
> **A Swiss cyber-security firm says it has accessed servers used by a hacking group tied to the SolarWinds breach, revealing details about who the attackers targeted and how they carried out their operation.** The firm, PRODAFT, also said the hackers have continued with their campaign through this month. **PRODAFT researchers said they were able to break into the hackers' computer infrastructure and review evidence of a massive campaign between August and March, which targeted thousands of companies and government organizations across Europe and the U.S**. The aim of the hacking group, dubbed SilverFish by the researchers, was to spy on victims and steal data, according to PRODAFT's report. **SilverFish carried out an "extremely sophisticated" cyber-attack on at least 4,720 targets, including government institutions, global IT providers, dozens of banking institutions in the U.S. and EU, major auditing/consulting firms, one of the world's leading COVID-19 test kit manufacturers and aviation and defense companies,** according to the report. "[The] hackers maintained regular working hours and were most active Monday to

Friday between the hours of 8 a.m. and 8 p.m., the report said. **The hackers operated servers in Russia and Ukraine, and shared some of the same servers as a notorious Russian criminal hacking group known as Evil Corp**."

The concerns from private industry reflect the history of the NSA paying for and collecting software exploits and code vulnerabilities to exploit in their own cyber-attacks against our nation's enemies. Unfortunately, the U.S. guided the world in cyberspace since the 1990's, but the recent theft of NSA hacking tools and espionage against the U.S. led to the release of "Zero Day" exploits to transnational criminals, state actors, and the public on the Dark Web. The most dangerous cyber weapons have been turned and pointed against our country. The Biden administration remains committed to regulation of the technology industry and forcing software companies to disclose and share all known vulnerabilities with their products to the government. The motivation for this forced sharing is to create more effective "resiliency" in networks that control our critical infrastructure by creating new coding standards for the tech industry.

Riley, Tonya, (Technology and cybersecurity policy researcher). "The Cybersecurity 202: NSA director says intelligence has a big blind spot: domestic Internet activity." ***Washington Post,*** 3-26-21, https://www.washingtonpost.com/politics/2021/03/26/cybersecurity-202-nsa-director-says-intelligence-has-big-blind-spot-domestic-internet-activity/#click=https://t.co/kg8XkfRoXH

A judge rejected a request by an ex-CIA employee to dismiss charges of leaking hacking tools**. A judge denied former CIA employee Joshua Schulte's bid to dismiss espionage charges** on the grounds that the grand jury that indicted him did not have enough Hispanic or Black individuals, Larry Neumeister of the Associated Press reports. A trial for Schulte, who is accused of leaking CIA hacking tools to WikiLeaks and has pleaded not guilty to all charges, is expected to begin in October after a jury deadlocked last year. **WikiLeaks' 2017 release of the hacking tools was one of the most significant leaks in the CIA's decades-long history and laid bare the agency's hacking and surveillance methods. The Biden administration is readying an executive order to require companies to disclose breaches to U.S. government clients. A draft version of the order would also require companies to keep more records for investigations of the breaches and work with federal agencies as they respond**, according to Reuters's Christopher Bing, Nandita Bose and Joseph Menn. The order could be made public as early as next week, they write. **The executive order comes as the Biden administration plans its responses to the devastating SolarWinds and Microsoft**

> **Exchange hacks.** A National Security Council spokeswoman told Reuters no decision has been made on the final content of the executive order. Anne Neuberger, the deputy national security adviser for cyber and emerging technology, previewed the executive order earlier this month, when the government was still primarily grappling with SolarWinds. Neuberger said at the time that **the executive order would "focus on building in standards for software, particularly software that's used in critical areas."**

In response to the Solar Winds attacks, the U.S. must act to create new protections to its networks and critical infrastructure. Private companies, including Microsoft, are calling on the government to assist in creating more robust defenses to cyber-attacks, instead of only focusing U.S. cyber policy on the development and use of OCO's against our enemies. An example is the recent electricity grid collapse in Texas demonstrates the weaknesses inherent in much of the critical infrastructure of our nation, and the vulnerability of citizens to the effects of a cyber-attack. A second failed cyber-attack on water treatment facilities in Florida creates a new nightmare for America. Every part of the public and private sector is currently vulnerable to attack (Gould, 2021).

The question is not should we act, it is how we should act in response to this growing threat. Congress needs to create a better system of intelligence sharing between the government and private technology companies, to help identify and neutralize coding errors and system vulnerabilities that our adversaries could exploit. The disorganized nature of our government's response to the latest attacks creates a need for swift action and new partnerships. The threat of Russian and Chinese cyber-attacks calls for bipartisan support that would strengthen U.S. cyber defenses. As it becomes evident, the current capabilities and bureaucracies within our government are not suited to meet the challenges that we face.

To address these growing cybersecurity issues, President Biden imposed sanctions on Russia as of April 15, 2021. In addition, our European allies and the U.S. are in joint agreement of deterring Russia's military presence in Crimea and Ukraine (Sanger, David E., and Andrew E.

Kramer, 2021). The question becomes when and how will Russia respond to these bilateral and multilateral reprimands?

II. Resolutions

1. The USFG should substantially increase its security cooperation with NATO in one or more of the following: artificial intelligence, biotechnology, cybersecurity.

2. NATO should substantially increase its security cooperation in one or more of the following: artificial intelligence, biotechnology, cybersecurity.

3. The USFG and NATO should substantially increase their security cooperation for one or more of the following: artificial intelligence, biotechnology, cybersecurity.

4. The USFG and NATO should substantially increase their policy cooperation in one or more of the following: artificial intelligence, biotechnology, cybersecurity.

5. The USFG and NATO should substantially increase their engagement in one or more of the following: artificial intelligence, biotechnology, cybersecurity.

6. The USFG and NATO should substantially increase their technology cooperation for one or more of the following: artificial intelligence, biotechnology, cybersecurity.

III. Definitions

Artificial Intelligence

The FY2019 National Defense Authorization Act (via Congressional Research Service, https://fas.org/sgp/crs/natsec/R45178.pdf) defines "artificial intelligence" as:

> **Almost all academic studies in artificial intelligence acknowledge that no commonly accepted definition of AI exists**, in part **because of the diverse approaches to research in the field**. Likewise, although Section 238 of the FY2019 National Defense Authorization Act (NDAA) directs the Secretary of Defense to produce a definition of artificial intelligence by August 13, 2019, **no official U.S. government definition of AI yet exists**. 6 **The FY2019 NDAA does, however, provide a definition of AI** for the purposes of Section 238: **1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. 2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. 3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks. 4. A set of techniques, including machine learning that is designed to approximate a cognitive task. 5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.7**

Britannica (https://www.britannica.com/technology/artificial-intelligence) defines "artificial intelligence" as:

> **Artificial intelligence (AI) is the ability of a computer or a robot controlled by a computer to do tasks that are usually done by humans because they require human intelligence and discernment.** Although there are no AIs that can perform the wide variety of tasks an ordinary human can do, some AIs can match humans in specific tasks.

IBM (https://www.ibm.com/cloud/learn/what-is-artificial-intelligence) defines "artificial intelligence" as:

> In computer science, the term artificial intelligence **(AI) refers to any human-like intelligence exhibited by a computer, robot, or other machine. In popular usage, artificial intelligence refers to the ability of a computer or machine to mimic the capabilities of the human mind**—learning from examples and experience, recognizing objects, understanding and responding to language, making decisions, solving problems—and combining these and other capabilities to perform functions a human might perform, such as greeting a hotel guest or driving a car.

General AI

The Congressional Research Service (https://fas.org/sgp/crs/natsec/R45178.pdf) defines "General AI" as:

> Experts generally agree that it will be many decades before the field advances to develop **General AI**, which **refers to systems capable of human-level intelligence across a broad range of tasks**.10 Nevertheless, the rapid advancements in Narrow AI have sparked a wave of investment, with U.S. venture capitalists raising an estimated $18.5 billion for AI research in 2019 alone. 11 Similarly, DOD's unclassified investments in AI have grown from just over $600 million in FY2016 to $2.5 billion in FY2021 (including investments in autonomy), with the Department reportedly maintaining over 600 active AI projects. 12

Narrow AI

The Congressional Research Service (https://fas.org/sgp/crs/natsec/R45178.pdf) defines "Narrow AI" as:

> The field of AI research began in the 1940s, but an explosion of interest in AI began around 2010 due to the convergence of three enabling developments: (1) the availability of "big data" sources, (2) improvements to machine learning approaches, and (3) increases in computer processing power.8 This growth has advanced the state of **Narrow AI**, which **refers to algorithms that address specific problem sets like game playing, image recognition, and navigation. All current AI systems fall into the Narrow AI category. The most prevalent approach to Narrow AI is machine learning, which involves statistical algorithms that replicate human cognitive tasks by deriving their own procedures through analysis of large training data sets.** 9 During the training process, the computer system creates its own statistical model to accomplish the specified task in situations it has not previously encountered.

Enterprise AI

NATO (https://www.nato.int/docu/review/articles/2020/11/24/artificial-intelligence-at-nato-dynamic-adoption-responsible-use/index.html) defines "Enterprise AI" as:

> Enterprise AI includes applications such as AI-enabled financial or personnel management systems, which are deployed in tightly controlled environments, where the implications of technical failures are low (in terms of immediate danger and potential lethality).

Operational AI

NATO (https://www.nato.int/docu/review/articles/2020/11/24/artificial-intelligence-at-nato-dynamic-adoption-responsible-use/index.html) defines "Operational AI" as:

> Operational AI, by contrast, can be deployed in missions and operations, i.e. in considerably less controlled environments and such that the implications of failure may be critically high. Examples include the control software of stationary systems or those of unmanned vehicles.

Mission Support AI

NATO (https://www.nato.int/docu/review/articles/2020/11/24/artificial-intelligence-at-nato-dynamic-adoption-responsible-use/index.html) defines "Mission Support AI" as:

Mission Support AI, an intermediate category in terms of environment control and failure implications, includes a diverse set of applications, e.g. logistics and maintenance, or intelligence-related applications.

Machine Learning

NATO (https://www.nato.int/docu/review/articles/2020/11/24/artificial-intelligence-at-nato-dynamic-adoption-responsible-use/index.html) defines "Machine Learning" as:

> The contemporary wave of AI, or Second Wave AI, is centered on Machine Learning (ML). ML involves the development and use of statistical algorithms to find patterns in data. For example, a classification algorithm can be trained on a large set of correctly labelled examples to determine to which previously encountered category a newly observed object belongs.

Deep Learning

NATO (https://www.nato.int/docu/review/articles/2020/11/24/artificial-intelligence-at-nato-dynamic-adoption-responsible-use/index.html) defines "Deep Learning" as:

> Deep Learning is a subset of ML, which uses multiple computational layers (Artificial Neural Networks with multiple layers) for the handling of computationally demanding pattern recognition or prediction problems, e.g. Convolutional Neural Networks for object detection within images.

Biotechnology

Biotechnology used to solve problems. ***Britannica*** defines "biotechnology" as:
https://www.britannica.com/technology/biotechnology

> Biotechnology, the use of biology to solve problems and make useful products. The most prominent area of biotechnology is the production of therapeutic proteins and other drugs through genetic engineering.

Biotechnology is a broad term
Dieuliis, Diane. "Biotechnology for the Battlefield: In Need of a Strategy." ***War on the Rocks***, 27 Nov. 2018, warontherocks.com/2018/11/biotechnology-for-the-battlefield-in-need-of-a-strategy/.

> Biotechnology — a broad term used to describe technological innovation based on biology —

Norweigan University of Science and Technology defines biotechnology
https://www.ntnu.edu/ibt/about-us/what-is-biotechnology

> **Biotechnology** is technology that **utilizes biological systems,** living organisms or parts of this to develop or create different products.

Biotechnology is an umbrella term for an ever expanding area of research
Hilgartner, Stephen. "Biotechnology." International Encyclopedia of the Social and Behavioral Sciences. **2001**. https://www.sciencedirect.com/science/article/pii/B0080430767031478

> **Defining biotechnology poses challenges, for the word is less a tightly-defined, technical term than a loose umbrella category**, or even a slogan, that conveys—sometimes simultaneously—visions of unbounded progress and unregulated tampering with nature. **Many authors have tried to capture biotechnology within their own well-crafted definitions, but these attempts cannot neatly contain this expanding network of activities and its increasingly dense connections to diverse social worlds**. Although the word has a long history (Bud 1993), **in most contemporary contexts biotechnology refers to a novel and growing collection of techniques, grounded in molecular and cell biology, for analyzing and manipulating the molecular building blocks of life**. The term also designates products, such as pharmaceuticals or genetically-modified foods, created using these techniques. At times, it refers not to products or techniques but to an economic sector or area of research.

Biotechnology often seen narrowly through the lens of security risk
Dieuliis, Diane. "Biotechnology for the Battlefield: In Need of a Strategy." *War on the Rocks*, 27 Nov. 2018, warontherocks.com/2018/11/biotechnology-for-the-battlefield-in-need-of-a-strategy/.

> **Biotechnology — a broad term used to describe technological innovation based on biology — has become an increasingly agile platform for developing new types of soldier enhancements. As such, the field offers novel opportunities for improving warfighter survivability on the battlefield**. Despite **recent developments**, however, **the Department of Defense has yet to strategically guide the development of these new technologies** at the national level. Recently, *War on the Rocks* published **an article outlining concerns** about the lack of coordinated policy for developing synthetic biology – a branch of biotechnology – while preventing its misuse by adversaries. The article rightly pointed to the need to think strategically about the risk of proliferating synthetic biology capabilities, but this is only one part of the picture. **Current national strategies encourage policymakers to view advances in biology through a narrow lens of risks to national security and the development of countermeasures to protect against those risks, which, while crucial, neglects the promise for using the same science to develop life-saving or other advanced tools for warfighters**. The Pentagon's current efforts to take advantage of synthetic biology as a platform for defense lack internal cohesion and external direction, and biological innovation faces further challenges given the absence of agile business models to fully harness emerging biotechnologies for the battlefield. **Greater coordination between those in the Defense Department whose work relates to biotechnology and improved relationships with the private sector are important first steps toward using this burgeoning area of science not just to mitigate security risks, but also to benefit soldiers on the battlefield.**

Agricultural biotechnology is internationally accepted and beneficial
https://www.state.gov/agricultural-policy/biotechnology/

> **As of 2019, genetically engineered crops were grown in 29 countries while 42 additional countries imported these crops.** Of the countries that grow biotech crops, ten are in

Latin America, six are in Africa, two in North America, two in Europe, and nine are in Asia and International acceptance will continue to grow as science-based, risk-proportionate regulations are developed regarding the cultivation and trade of biotech crops and people experience the benefits. However, **widespread misunderstanding persists about this technology, its safety, and the breadth of its potential.** Foods derived through advanced agricultural technology undergo extensive risk assessment procedures by a variety of national bodies such as the Environmental Protection Agency, the United States Department of Agriculture, and the Food and Drug Administration. **Biotech crops also undergo analysis by international entities such as the European Food Safety Agency**. Any biotech crops approved by these bodies have been designated as safe for both people and the environment. **International acceptance will continue to grow as science-based regulations are developed regarding the cultivation and trade of biotech crops and people experience the benefits.**

Cybersecurity

Digital Guardian *defines "cyber security" as:*

https://digitalguardian.com/blog/what-cyber-security

> **Cyber security** refers **to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access**. **Cyber security may also be referred to as information technology security.** **Oct 5, 2020**

https://csrc.nist.gov/glossary/term/cybersecurity

> **The process of protecting information by preventing, detecting, and responding to attacks**. Source(s): NISTIR 8183 under **Cybersecurity NIST Cybersecurity** Framework Version 1.1, **NIST Cybersecurity** Framework Version 1.0.

https://www.merriam-webster.com/dictionary/cybersecurity

> Definition of ***cybersecurity***
> **:** measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

https://searchsecurity.techtarget.com/definition/cybersecurity

> **Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats**. **The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.**
> A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data.
> **Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations**.

https://www.forcepoint.com/cyber-edu/cybersecurity

> Also referred to as information security, **cybersecurity refers to the practice of ensuring the integrity, confidentiality, and availability (ICA) of information**. **Cybersecurity is comprised of an evolving set of tools, risk management approaches, technologies, training, and best practices designed to protect networks, devices, programs, and data from attacks or unauthorized access.**

Engagement

https://www.collinsdictionary.com/dictionary/english/engagement

> An **engagement** is an arrangement that you have made to do something at a particular time.

https://www.oxfordlearnersdictionaries.com/us/definition/english/engagement

> an arrangement to do something at a particular time, especially something official or something connected with your job

https://www.definitions.net/definition/military+engagement

military engagement

> Routine contact and interaction between individuals or elements of the Armed Forces of the United States and those of another nation

https://www.collinsdictionary.com/dictionary/english/engagement

> A military **engagement** is an armed conflict between two enemies.
> *The constitution prohibits them from military engagement on foreign soil.*

NATO

https://kevtellier.substack.com/p/march-29-2021-reading-notes-ryan

> **North Atlantic Treaty Organization:** an organization formed in Washington, D.C. (1949), comprising the 12 nations of the Atlantic Pact together with Greece, Turkey, and the Federal Republic of Germany, for the purpose of collective defense against aggression.

https://www.thebalance.com/nato-purpose-history-members-and-alliances-3306116

> The North Atlantic Treaty Organization (NATO) is an alliance of 30 countries that border the North Atlantic Ocean. The Alliance includes the United States, most European Union members, the United Kingdom, Canada, and Turkey.

https://www.collinsdictionary.com/us/dictionary/english/nato

NATO is an international organization which consists of the U.S., Canada, Britain, and other European countries, all of whom have agreed to support one another if they are attacked. **NATO** is an abbreviation for 'North Atlantic Treaty Organization.'

Policy

https://www.dictionary.com/browse/policy

a course of action adopted and pursued by a government, ruler, political party, etc.:*our nation's foreign policy.*

https://legal-dictionary.thefreedictionary.com/Policy

As applied to a law, ordinance, or **Rule of Law**, *the general purpose or tendency considered as directed to the welfare or prosperit of the state or community.*

Cooperation

https://link.springer.com/chapter/10.1057/9780230372214_2

What do international relations scholars understand by the term 'cooperation'? Whereas realists and neoliberals disagree about the importance of international cooperation, there is widespread agreement on a working definition.1 Cooperation arises, 'when actors adjust their behaviour to the actual or anticipated preferences of others, through a process of policy coordination'.2

https://www.merriam-webster.com/dictionary/cooperation

: the actions of someone who is being helpful by doing what is wanted or asked for **:** common effort. We are asking for your full *cooperation.*

https://link.springer.com/chapter/10.1057/9780230372214_2

What do **international relations** scholars understand by the term '**cooperation**'? ... **Cooperation** arises, 'when actors adjust their behaviour to the actual or anticipated preferences of others, through a process of policy coordination'.

Foreign Policy Cooperation

https://www.britannica.com/topic/foreign-policy

Foreign policy, general objectives that guide the activities and relationships of one state in its interactions with other states. The development of **foreign policy** is influenced by domestic considerations, the **policies** or behaviour of other states, or plans to advance specific geopolitical designs.

"The Emergence of Foreign Policy Halvard Leira." ***International Studies Quarterly***, Volume 63, Issue 1, March 2019, Pages 187–198, accessed on 05 February 2019 https://academic.oup.com/isq/issue/63/1

> The discipline of international relations offers **two different takes on "foreign policy."** First, **it sees foreign policy as carrying a self-evident meaning: as an abstract expression of relations between political entities: "Broadly interpreted, foreign policy is about the fundamental issue of how organized groups, at least in part strangers to each other, interrelate"** (Hill 2003, xvii). **Such definitions render foreign policy as an analytic concept that transcends particular historical periods or kinds of political communities.** It is always distinct, and essentially different, from other forms of policy. **Second, critics of this account suggest that foreign policy provides one of the key ways in which the political Self is differentiated from the Other: "Foreign policy was not a bridge between two distinct realms, but something that both divided and joined the inside and the outside, the state and the interstate system"** (Campbell 1998, 60). In this understanding, foreign policy emerged sometime during the seventeenth century. **It was producer, and the product, of the modern state and state system.**

https://study.com/academy/lesson/cooperation-among-states-political-military-economic-alliances.html#:~:text=Being%20more%20of%20a%20concept,the%20deciding%20of%20territorial%20boundaries.

> Being more of a concept than a term, political cooperation broadly denotes the governments of differing states working together toward a common goal. This cooperation can occur in areas like military alliances, economic affairs, and the deciding of territorial boundaries.
>
> Probably one of the most famous examples of political cooperation is the United Nations. Formed after World War II, the United Nations is an intergovernmental organization tasked with the job of promoting and maintaining political cooperation among the world's nations.

https://oxfordre.com/internationalstudies/internationalstudies/abstract/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-93

> The study of international cooperation has emerged and evolved over the past few decades as a cornerstone of international relations research. Our strategy for reviewing such a large literature is to focus primarily on the rational choice and game theoretic approaches that instigated it and have subsequently guided its advance. Without these theoretical efforts, the study of international cooperation could not have made nearly as much progress—and it certainly would not have taken the form it does in the 21st century. Through this lens, we identify major themes in this literature and highlight key challenges for future research.
> This definition of international cooperation is general in terms of both actors and issues. Cooperation occurs not only among individuals but also among collective entities, including firms, political parties, ethnic organizations, terrorist groups, and nation-states. Although ICT often defines international cooperation in terms of states, it can also involve other actors, especially intergovernmental organizations (IGOs) and

nongovernmental organizations (NGOs). These diverse actors cooperate for different objectives across a wide range of issue areas: IGOs work with states to combat global environmental problems, firms collude to monopolize markets, NGOs campaign to save the whales, and so on. Finally, international cooperation is not always a good thing, at least from the perspective of those excluded or targeted. For example, international sanctions involve cooperation against target countries (Martin, 1992a; Drezner, 1999), and commodity cartels often harm consumer states.

Cooperation is supported in repeated settings because of the possibility of reciprocity: if you cooperate with me, then I will cooperate with you in the future; but if you do not cooperate, then neither will I. If both actors take this position—as in the famous tit-for-tat strategy pairing—then ongoing cooperation is supported against current defection incentives by actors' interest in maintaining cooperation into the future. This analysis opens up the possibility of cooperation and raises interesting questions regarding the conditions under which strategies of reciprocity promote cooperation. Parallel empirical work (e.g., Goldstein, 1991; Ward & Rajmaira, 1992; Goldstein & Pevehouse, 1997) has shed important light on these conditions.

Foreign Policy

https://marketbusinessnews.com/financial-glossary/foreign-policy/

foreign policy or **foreign relations** refers to how a government deals with other countries. ... The government chooses its **foreign affairs policy** to safeguard the interests of the nation and its citizens. 'Trade,' in this context, means 'international trade,' i.e., imports, exports, tariffs, exemptions, etc.

https://www.britannica.com/topic/foreign-policy

Foreign policy, general objectives that guide the activities and relationships of one state in its interactions with other states. The development of foreign policy is influenced by domestic considerations, the policies or behaviour of other states, or plans to advance specific geopolitical designs. Leopold von Ranke emphasized the primacy of geography and external threats in shaping foreign policy, but later writers emphasized domestic factors. Diplomacy is the tool of foreign policy, and war, alliances, and international trade may all be manifestations of it.

https://www.dictionary.com/browse/foreign-policy

noun

a policy pursued by a nation in its dealings with other nations, designed to achieve national objectives.

Engagement

https://www.merriam-webster.com/dictionary/engagement

Definition of *engagement*

1a
: an arrangement to meet or be present at a specified time and place

https://www.weforum.org/agenda/2015/04/why-engagement-is-the-key-to-us-foreign-policy/

> From the beginning, however, the Obama administration has made clear that engagement is not an end in itself, but a means to various goals, both bilateral and regional.
>
> Another source of doubt about America's enduring influence lies in the fact that multilateral engagement is still needed, and this is always more difficult than bilateral engagement. Indeed, multilateral leadership requires not only clearer and bolder rules, but also a demonstrated willingness to bear the costs of those rules, whether by creating safe zones to uphold the "responsibility to protect" civilians or taking concrete steps to reduce – and eventually eliminate – nuclear arsenals.
>
> Bilateral engagement will prove to be one of Obama's most important foreign-policy legacies. But ensuring that the US can continue to lead in the twenty-first century will require a different kind of engagement. That will be a critical task for America's next president.

https://www.state.gov/a-foreign-policy-for-the-american-people/

> Over the decades, these commitments have created new markets for our products, new allies to deter aggression, and new partners to help meet global challenges. We had a name for it: "enlightened self-interest." We'll be clear that real partnership means carrying burdens together, everyone doing their part – not just us. And whenever we can, we will choose engagement. Wherever the rules for international security and the global economy are being written, America will be there, and the interests of the American people will be front and center.

Security

https://globalsecurityreview.com/what-is-security-everything/

> Security is an inherently contested concept, encompassing a wide variety of scenarios, and is commonly used in reference to a range of personal and societal activities and situations.
> Security can be distinguished between day-to-day security at the individual level (nutritional, economic, safety), security for favorable conditions (the rule of law and due process, societal development, political freedom), and security against adverse conditions or threats (war and violence, crime, climate change).
> The term security is used in three broad segments. The first is the general, everyday use of the term. In this instance, security refers to the desire for safety or protection. Second is the usage of the word for political purposes; relating to political processes, structures, and actions utilized to ensure a given political unit or entity is secure. The term "security" is frequently used as a political tool to assign priority to a given issue or perceived threat within the broader political realm.

> Third, and finally, "security" can be employed as an analytical concept to identify, define, conceptualize, explain, or forecast societal developments such as security policy, institutions, and governance structures.

https://www.researchgate.net/publication/303899299_Concept_of_Security

> Fundamentally, **security** has to do with the presence of peace, safety, gladness and. the protection of human and physical resources or absence of crisis or threats to. human dignity, all of which facilitate development and progress of any human. society. The **concept of security** has become a preoccupation for the decades.

https://www.peacepalacelibrary.nl/ebooks/files/370659244.pdf

> Until fairly recently, the term 'security' was almost monopolized by the academic discipline of International Relations (IR). IR theorists employed it in a rather narrow sense which happened to correspond to the way politicians tended to use the word, i.e. as almost synonymous with military power. The more military power, or rather the more favourable the military balance, the more security. Surprisingly little was, however, written about security by the IR theoreticians, in the works of whom 'national interest' and/or 'power' were preferred, sometimes as alleged synonyms of security. In his seminal work on Realism, Hans Morgenthau thus hardly bothered to define 'security'ii. Arnold Wolfers was one of the few who ventured a definition of the term: 'security, in an objective sense, measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values will be attacked.'iii

Security Cooperation

https://www.defense.gov/Explore/News/Article/Article/2048832/defense-department-begins-security-cooperation-workforce-program/

> **Security cooperation** is the effort to advance U.S. national **security** and foreign policy interests by building the capacity of foreign **security** forces to respond to shared challenges.

https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_20_20172305.pdf

> **Security cooperation** (SC) encompasses all Department of Defense (DOD) interactions, programs, and activities with foreign security forces (FSF) and their institutions to build relationships that help promote US interests; enable partner nations (PNs) to provide the US access to territory, infrastructure, information, ...May 23, 2017

https://www.dscu.mil/documents/publications/greenbook/01_Chapter.pdf?id=1

> **Security cooperation** (SC) encompasses all Department of **Defense** (DOD) interactions, programs, and activities with foreign **security** forces (FSF) and their institutions to build relationships that help promote US interests; enable partner nations (PNs) to provide the US access to territory, infrastructure, information,....

https://www.dau.edu/cop/iam/Pages/Topics/Security%20Cooperation.aspx

> DoD **Security Cooperation** is defined in Joint Pub 1-02: All DoD interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation. **DoD Directive 5132.03** provides DoD-wide policy and describes DoD organizational responsibilities regarding Security Cooperation activities.
>
> DoD Security Cooperation includes **International Armaments Cooperation (IAC)** activities as well as the various elements of **Security Assistance**, including **Foreign Military Sales (FMS)** and **Building Partner Capacity (BPC).** Most DoD **Security Cooperation** policy, organization, and activities (other than IAC) are led and managed by USD(Policy) rather than USD(Acquisition & Sustainment) and USD(Research & Engineering), but many U.S. Government/DoD Security Cooperation activities are implemented through USD(A&S), USD(R&E), and DoD Component acquisition-related IA&E efforts.
>
> The primary source of day-to-day guidance on Security Assistance and BPC policies and practices is the Defense Security Cooperation Agency (DSCA)-issued Security Assistance Management Manual (eSAMM). FMS transactions are implemented through FMS Letters of Offer and Acceptance (LOAs), often referred to as "FMS cases." BPC transactions are normally referred to as "pseudo-FMS cases."

https://www.thefreedictionary.com/security+cooperation

> All Department of Defense interactions with foreign defense establishments to build defense relationships that promote specific US security interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide US forces with peacetime and contingency access to a host nation. See also security assistance; security assistance organization.

policy cooperation

Cœuré, Benoît (Member of the Executive Board of the ECB, at the Global Research Forum on International Macroeconomics and Finance, Washington D.C.), ***European Central Bank***, S14 November 2014
https://www.ecb.europa.eu/press/key/date/2014/html/sp141114.en.html
For a central banker from the euro area, the notion of policy coordination and cooperation has a somewhat different meaning than it does for policymakers from other advanced economies. On the one hand, it has a global dimension capturing the difficult questions of whether and how to align monetary policies so as to achieve an optimal international policy mix. But on the other hand, it has a meaning as well in our domestic environment: within the euro area we are also involved, in a sense, in international policy cooperation. We have to achieve price stability in an environment of different national fiscal and structural policies.

technology

https://languages.oup.com/google-dictionary-en/

noun

1. the application of scientific knowledge for practical purposes, especially in industry.

"advances in computer technology"

- machinery and equipment developed from the application of scientific knowledge. "it will reduce the industry's ability to spend money on new technology"
- the branch of knowledge dealing with engineering or applied sciences.

https://www.britannica.com/technology/technology

Technology, the application of scientific knowledge to the practical aims of human life or, as it is sometimes phrased, to the change and manipulation of the human environment.

https://www.merriam-webster.com/dictionary/technology

Technology (*noun*):

1) (a): the practical application of knowledge especially in a particular area; (b): a capability given by the practical application of knowledge
2) a manner of accomplishing a task especially using technical processes, methods, or knowledge.
3) the specialized aspects of a particular field of endeavor.

Hughes, Thomas. ***Human-Built World: How to Think about Technology and Culture***. 2004.
https://techliberation.com/2014/04/29/defining-technology/

"Technology is messy and complex. It is difficult to define and to understand. In its variety, it is full of contradictions, laden with human folly, saved by occasional benign deeds, and rich with unintended consequences." (p. 1) "Defining technology in its complexity," he continued, "is as difficult as grasping the essence of politics." (p. 2)

Thomas Hughes' definition:

"a creativity process involving human ingenuity." (p. 3)

Arthur, W. Brian. ***The Nature of Technology: What It Is and How It Evolves***. 2009.
https://techliberation.com/2014/04/29/defining-technology/

1) "The first and most basic one is a technology is *a means to fulfill a human purpose*. … As a means, a technology may be a method or process or device… Or it may be complicated… Or it may be material… Or it may be nonmaterial. Whichever it is, it is always a means to carry out a human purpose."

2) "The second definition is a plural one: technology as an *assemblage of practices and components*."
3) "I will also allow a third meaning. This technology as the entire *collection of devices and engineering practices available to a culture*." (p. 28, *emphasis in original*.)

https://brainly.com/question/1406047

> The best definition of technology is the study and transformation of techniques, tools, and machines created by humans. Technology allows humans to study and evolve the physical elements that are present in their lives.

https://www.researchgate.net/publication/320571654_A_Comprehensive_Definition_of_Technology_from_an_Ethological_Perspective

> Definitions, uses, and understanding of technology have varied tremendously since Jacob Bigelow's Elements of Technology in 1829. In addition to providing a frame of reference for understanding technology, the purpose of this study was to define or describe it conceptually. A determination of dimensions comprising technology was made by critiquing historical and contemporary examples of definition by Bigelow and Volti. An analytic-synthetic method was employed to deconstruct both definitions spanning two centuries to derive aspects of technology. Definitions relying on an anthropocentric "how humans use technology" viewpoint failed to account for different perspectives that were found when an ethological perspective inquiring "how technology is used" served as a framework. **Findings support qualification of insulin as technology according to the following comprehensive definition: something inherently intelligent enough to either function, be used to function, or be interpreted as having a function that intelligent beings—human or otherwise—can appreciate, something devised, designed (by primary intention), or discovered (by secondary intention) serving particular purposes from a secular standpoint without humankind creating it, or a significant beneficiary of rationally derived knowledge that is "used for" a purpose without itself necessarily being translated into something material that "does" autonomously, or dependently when used.**

technology cooperation

Philibert, Cedric (International Energy Agency). "International Energy Technology Collaboration And Climate Change Mitigation." International Energy Agency. **2004**.
https://www.oecd.org/env/cc/32138947.pdf

> "All countries are interested in being leaders in technology development – if not for protecting the climate, at least for competitive concerns. Therefore, one may think of technology cooperation as a way to engage more countries into action (or into more action)."

Arranz, Nieves (Faculty of Economics and Business Administration) and Juan C. Fdez. de **Arroyabe** (ESIC Business & Marketing School). "Technological Cooperation:
A New Type of Relations in the Progress of National Innovation Systems." The Innovation Journal: The Public Sector Innovation Journal. **2009**.
https://www.innovation.cc › scholarly-style › 2009_14_2…

> We can define **technological cooperation** as the agreement between two or more independent agents who, by joining or sharing their skills and/or resources, develop and carry out a **technological** process with the aim of increasing their competitive advantages. The resulting type of agreement will depend on the contingencies of the environment, the characteristics of the item to be transferred, the qualities and behaviour of the contracting agents, etc. and therefore numerous contractual arrangements will exist (Gulati, 1998).

United Nations Industrial Development Organization and the World Business Council for Sustainable Development. "Developing Countries and Technology Development." **2002**. https://www.wbcsd.org/contentwbc/download/2337/29341

> Technology cooperation requires longer-term partnerships in which all parties have a vested interest in successful continuing operation. It requires incorporating both the "hardware" technology components and the equally essential range of "software" components. Both components are necessary to ensure a continuing stream of economic benefits that accrue fairly to all partners. This includes process machinery and equipment, as well as patented and unpatented manufacturing techniques and production knowhow. This can also include, more broadly, managerial, organizational, and marketing knowledge that contribute to the development of new skills.

IV. Timeliness

For most of 2020, U.S. citizens were consumed with the pandemic, election fraud, and police tactics. However, with the new Biden administration, our lens is trained on not just domestic problems, but geopolitical relationships and daunting hotspots or potential crises. For example, with the recent AI creation of humanlike robots, use of biotechnology for vaccines, and cybersecurity breach of Colonial Pipelines and SolarWinds, our government is facing threats from Russia and China to become the leaders of emerging technologies. President Biden visualizes opportunities to reaffirm, to our allies, our commitment to stave off potential crises. He is now attempting to correct the foreign policy mistakes of the former administration and hold foreign countries accountable for their actions. But, this administration must repair its rapport with allies to be able to exert collaborative efforts in maintaining world peace regarding the development and use of AI, biotechnology, and cybersecurity.

V. Scope

Artificial intelligence, biotechnology, and cybersecurity impact the daily lives of every American. Thus, the threats posed by each of these dual-use technologies is of critical significance in all sectors of the country. Artificial intelligence has the power to make our work more efficient and empower our enemies. Improved biotechnology capability could revolutionize medicine and at the same time could be used to devastate crops or directly attack the health of the American public with an engineered biological agent. Cybersecurity experts must constantly balance how to develop countermeasures toward other countries while also shoring up potential risks to our own systems. Protecting the ability of science to mature in a way that enables innovation, encourages economic growth, maintains security, and encourages diplomacy is vital to the long-term goals of the entire country.

VI. Range

Artificial Intelligence--AI

Affirmative Ground

In making the case that the U.S. and NATO should cooperate on AI against the backdrop of rising AI competition, affirmative teams would be able to draw on a substantial body of research and analysis arguing for greater transatlantic collaboration on AI strategy. Specifically, experts have pointed to the digital, physical, and political security issues posed by AI as ripe for more NATO cooperation.

> **Kasapoglu,** Can (the director of the defense and security program at the Istanbul-based think-tank EDAM. D) **and** Baris **Kirdemir** (edam non-resident fellow).
> "Artificial Intelligence and the Future of Conflict." ***Carnegie Europe,*** November 28, 2019, https://carnegieeurope.eu/2019/11/28/artificial-intelligence-and-future-of-conflict-pub-80421
>
> **NATO would benefit from a convergence of transatlantic regulatory and legislative frameworks to better steer the trajectory of the coming transformation.** In 2018, a

consortium of U.S. and European experts from industry, civil society, and research institutions published a report that outlined three areas of concern.12 **The first is the digital security domain, in which the report warned of potential AI vulnerabilities that would allow adversaries to stage large-scale, diversified attacks on physical, human, and software targets.**

Second, **in the physical security domain, the availability and weaponization of autonomous systems cause major challenges. Cyber and physical attacks on autonomous and self-driving systems and swarm attacks—coordinated assaults by many agents on multiple targets—are other potential threats.**

Third, there are significant risks to political security. AI-enabled surveillance, persuasion, deception, and social manipulation are threats that will intensify in the near future. New AI capabilities may strengthen authoritarian and discriminatory political behavior and undermine democracies' ability to sustain truthful public debates.

NATO leaders themselves have signaled that they're open to more cooperation on AI.

"Cooperation on Artificial Intelligence will boost security and prosperity on both sides of the Atlantic, NATO Deputy Secretary General says." ***NATO,*** October 28, **2020**, https://www.nato.int/cps/en/natohq/news_179231.htm

"**There are considerable benefits of setting up a transatlantic digital community cooperating on Artificial Intelligence (AI) and emerging and disruptive technologies, where NATO can play a key role as a facilitator for innovation and exchange**", said NATO Deputy Secretary General Mircea Geoană. On Wednesday (28 October 2020) he took part in a high-level virtual discussion on transatlantic cooperation in the era of AI, organised by the Atlantic Council's Future Europe Initiative and GeoTech Center.

…

"NATO is a natural platform for transatlantic cooperation of AI," the Deputy Secretary General underlined. "NATO offers its consultative mechanisms and unique networks for collaboration on defence and security questions. Bringing together Allies and partners, public and private sector, innovators and industry. We have great communities in areas like military capability development, science and technology, standardisation - and of course our Command Structure and military exercises. We also have new cross-cutting policy teams on Innovation Policy, who cover AI, and on Data Policy," he pointed out.

Moreover, NATO is uniquely positioned to address the complex challenges posed by emerging technologies, boasting defense capabilities, technological prowess, and an organizational infrastructure well-suited to the new global reality.

Stavridis, James (ADM **James** G. **Stavridis**, former Commander, EUCOM, and NATO Supreme Allied Commander Europe). "Why NATO Is Essential For World Peace, According to Its Former Commander." ***Time,*** April 4, **2019**, https://time.com/5564171/why-nato-is-essential-world-peace/

For all those harbingers of trouble, though, by many traditional measures, **NATO remains extremely healthy.**
It is powerful. **The 29 nations of NATO produce more than 50% of the world's gross domestic product, have well over 3 million troops on duty, operate massive combined naval fleets and air forces and together spend over $1 trillion on defense**.
Indeed, even with all the frustration over European defense spending not hitting the 2% of GDP goal, the collective European defense budget is the second largest in the world after the U.S.'s and is ahead of China's and Russia's–combined.
It is smart. **U.S. and European defense innovation and production provides a formidable military research and development capacity. Particularly in cybersecurity, unmanned vehicles, space operations, special-forces technologies, maritime and anti-submarine capability, and air and missile defense, NATO is a technology and education superpower.**
It is capable. **The alliance boasts a large command structure of highly qualified teams of military officers from all of the 29 nations. Throughout Europe and the East Coast of the U.S., those teams prepare war plans, conduct training exercises, monitor readiness of allied units, gather intelligence about potential adversaries and run complex operations centers that cover the entire geographic range of NATO**.
These standing staffs, which we rationalized by reducing them 35% while I was NATO commander, can conduct prompt and sustained combat operations in a coalition structure on short notice.

In terms of advantages, affirmatives have much fertile ground to plow. On the economy, for example, teams can point to analyses that international competition can act as a great accelerant for economic innovation and growth (much as the U.S. competition with the Soviet Union for space supremacy spurred a wide range of technological advances beyond the space race itself).

Allison, Graham (Douglas Dillon Professor of Government, Harvard Kennedy School Member of the Board, Belfer Center, Former Director, Belfer Center) **and** Eric **Schmidt** (former CEO of Google and a former executive chairman of Google and Alphabet, is Chair of the US National Security Commission on Artificial Intelligence). "Is China Beating the U.S. to AI Supremacy?" ***Belfer Center,*** August **2020**, https://www.belfercenter.org/publication/china-beating-us-ai-supremacy

First, Americans must wake up to the challenge. Recognition that that the United States faces a serious competitor in a contest in which the outcome will be decisive for our future is necessary to get our competitive juices flowing. The Olympics offers an instructive analogy for thinking about a competitive strategy for AI. It also reminds us that competition is inherently a good thing. **Competition produces superior performance. Participants in a marathon run faster than they do when running alone. Indeed, competition is a core American value. Free markets organize a competitive process that produces better products at cheaper prices. Science and its applications advance as research teams compete to better understand the world.**

Additionally, affirmatives can argue advantages such as U.S. hegemony/global leadership, international cooperation, nuclear war prevention – some experts have warned that unchecked AI could pave the way to automated nuclear attacks (Straub, 2018) – national security, and more.

Negative Ground

Negative teams would have a rich array of options for countering the affirmative. For example, experts have pointed to divergent U.S. and European interests on AI policy, which could hinder effective transatlantic cooperation.

> **Soare**, Simona R. (Sr. Assoc. Analyst @EUISS, focusing on US security policy, transatlantic security and EU-NATO relations). "Digital Divide? Transatlantic defence cooperation on Artificial Intelligence." ***ISS European Union Institute for Security Studies,*** March **2020**, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%203%20AI_0.pdf
>
> **The trouble is that Europeans have a different perspective on AI than Washington.29 Perhaps with the exception of France,30 Europeans view AI primarily through a geo-economic lens – as directly connected to their economic competitiveness.** Many in Europe feel that, if left unaddressed, the European digital and AI technology gap will transform Europe into a 'digital colony'.31 Reinforced by the White House's transactional approach, by European concerns over their own competitiveness in the digital economy, and by Brussels' fears of being pushed to the margins of US-China AI competition, there are pressing calls for Europe to defend its 'digital sovereignty.'32 Others believe Europe has a strategic opportunity to advocate a veritable 'third way' on AI.33 The European Commission's 'digital package' (released on 19 February) arguably goes a long way in this direction.
>
> Second, **this suggests that a significant structural shift in the partnership is emerging. As President Macron has argued, the challenge in this technological competition is tied to sovereignty: 'The battle we're fighting [on AI] is one of sovereignty … If we don't build our own champions in all new areas – digital, artificial intelligence – our choices... will be dictated by others.'34 The implication is that Europe's digital vulnerability is becoming a geopolitical security problem, reinforced by pre-existing European dependencies, not least in defence. The expectation is that the US should help its European partners remain strategically relevant in the arena of great power competition in the new digital era.**

U.S. and European perspectives also differ on China, suggesting that it may be difficult for the U.S. to rally its NATO allies behind an AI policy that will at least implicitly challenge China. Germany, for example, has been a force for increased economic ties with China.

Vela, Jakob Hanke (trade reporter for POLITICO), Giorgio **Leali** (policy reporter for POLITICO), **and** Barbara **Moens** (Trade Reporter at POLITICO), "Germany's drive for EU-China deal draws criticism from other EU countries." ***Politico,*** January 1, **2021**, https://www.politico.eu/article/germanys-drive-for-eu-china-deal-draws-criticism-from-other-eu-countries/

German Chancellor Angela Merkel's strong push to conclude the EU-China deal in the last days of the year has left a bad aftertaste among a group of EU countries who said they felt ignored.

Officials from Italy, Poland, Belgium and Spain criticized the way Germany pushed through the investment agreement with China in the final days of the German presidency of the Council of the EU, despite their warnings that the timing was tone deaf to slave labor concerns in China and risked alienating incoming U.S. President Joe Biden.

The officials said they felt steamrolled by Merkel and the "German engine" inside the European Commission, in particular Commission President Ursula von der Leyen and trade department director Sabine Weyand, who are both German.

"There's a lot of frustration among smaller countries about the way the Commission has been used to push through one of Merkel's pet projects at the end of her term and the end of her legacy," said one EU diplomat.

"Is this the way the EU will work post-Brexit? The Brits are just out and we're already missing their open market-oriented approach," the diplomat said. "If Germany weighs in too much, smaller EU countries have nothing to say."

The EU on Wednesday sealed a bilateral investment pact with China, allowing investors to acquire companies in a number of sectors, limiting joint venture requirements and allowing foreign employees to work in their respective markets.

But the critics worried that the deal was a political win for Chinese President Xi Jinping and came just as his government cracked down on democracy in Hong Kong, ethnic minorities in Xinjiang and journalists reporting on the origins of the coronavirus pandemic.

Disparate capabilities and interoperability challenges among member-states could also make a cohesive NATO AI strategy difficult.

Pepe, Erica (Recruitment Evangelist with the Employer Insights Team), "NATO and collective thinking on AI." ***IISS Blog,*** November 13, **2020,** https://www.iiss.org/blogs/military-balance/2020/11/nato-artificial-intelligence

In some ways NATO might seem a natural forum for these deliberations, not least in a transatlantic context. It also has a lot of experience, going back to the Cold War, in working towards standardisation and interoperability among allies. **However, the results achieved have been mixed, which underscores the challenges the Alliance now faces: not only 30**

members with disparate levels of capability, but also a backdrop of rapid technological advances where some of its competitors and potential adversaries may hold significant advantages. Interoperability issues may be thorny, but they need to be resolved if AI-dependent capability gaps between members are not to widen. Early discussions regarding the establishment of common technical standards on **the design and development of military-applicable AI would at least reduce this risk.**

Given NATO's potential pitfalls, negatives can offer alternative agent counterplans, including, but not limited to a unilateral U.S. approach; the United Nations; a bilateral agreement between the U.S. and China; and more.

What is more, negative teams can point to the issue of non-state actors exploiting AI, which underscores how a state-based approach to AI won't solve all concerns arising from its security implications.

Straub, Jeremy **(**Assistant Professor in the Department of Computer Science at the North Dakota State University). "Artificial intelligence is the weapon of the next Cold War." ***The Conversation,*** January 29, **2018,** https://theconversation.com/artificial-intelligence-is-the-weapon-of-the-next-cold-war-86086

Countries might agree to a proposed Digital Geneva Convention to limit AI conflict. But that won't stop AI attacks by independent nationalist groups, militias, criminal organizations, terrorists and others – and countries can back out of treaties. It's almost certain, therefore, that someone will turn AI into a weapon – and that everyone else will do so too, even if only out of a desire to be prepared to defend themselves.

An alternative would be to argue that the discourse around AI as a security threat is overblown. Fears of killer robots, for example, have been dismissed by many experts.

Berlatsky, Noah **(**Blog Editor at Prostasia Foundation). "Is AI dangerous? Why our fears of killer computers or sentient 'Westworld' robots are overblown**.**" ***NBC News***, **December 6,** 2018, https://www.nbcnews.com/think/opinion/ai-dangerous-why-our-fears-killer-computers-or-sentient-westworld-ncna943111

Malevolent robots are fun monsters, like vampires or aliens. But, like vampires and aliens, they're not real, according to "The AI Delusion," a new book by Pomona College Economics professor Gary Smith. **According to Smith, computers aren't smart enough to threaten us — and won't be for the foreseeable future. But if we think computers are smart, we may end up harming ourselves not in the far future, but right now.**
Computers seem more intelligent than us because they can perform certain tasks much better than we can. "People see computers do amazing things, like make complicated mathematical calculations and provide

> directions to the nearest Starbucks, and they think computers are really smart," Smith told me in a phone interview. Computers can memorize huge amounts of information — a computer has effectively solved the game checkers, calculating every possible move, so that it is unbeatable. If computers can beat humans in games of skill and intelligence, then computers must be more intelligent than humans are. And if they are more intelligent than us, it follows that they pose a danger to us. Right?
>
> **This reasoning is not right, according to Smith. Computers can calculate and memorize, but that doesn't mean they're smarter than humans. In fact, computers are, in most respects, no smarter than a chair. They don't have wisdom or common sense. "They have no understanding of the real world," Smith says.**

Additionally, negatives can put forward disadvantages including the economy, by pointing to research indicating that excessive state involvement in technology policy could constrain innovation and undermine U.S. economic competitiveness; China relations, arguing that an aggressive, security-based approach to countering China on AI could make greater conflict a fait accompli; and numerous tradeoff disadvantages, given that increased international cooperation on AI could detract focus from other critical challenges, including climate change, food insecurity, democracy and human rights, and more.

There is also an abundance of Kritik ground for negatives to explore. Negatives can attack the securitized rhetoric employed to discuss AI in the global arena; argue Kritiks including racism or Orientalism; make Capitalism Kritiks, given how much of what is at stake in the global AI competition are profits for major technology companies and government contracts for tech firms; and more.

Biotechnology

Affirmative Ground

In the early 2000's, bioterrorism was a hot topic. The images of the 9/11 attacks were fresh in the minds of Americans when purported anthrax attacks began appearing in the news the week after the World Trade Center towers were hit. This incident made the idea of a biological attack on American soil tangible. Since that time, scientific advances in biotechnology have

evolved. Gene editing presents the possibility that terrorists could design a deadly pathogen from organic or synthetic materials.

> **West**, Rachel M. (Postdoctoral Associate at the Johns Hopkins Center for Health Security and the Johns Hopkins Bloomberg School of Public Health), and Gigi Kwik **Gronvall** (Senior Scholar at the Johns Hopkins Center for Health Security and an Associate Professor in the Department of EHE), "CRISPR Cautions: Biosecurity Implications of Gene Editing." ***Perspectives in Biology and Medicine,*** vol. 63, no. 1, **2020**, pp. 73–92., doi:10.1353/pbm.2020.0006.
>
> **The potential for CRISPR to revolutionize genetic engineering also raises concerns that it could increase biosecurity threats by lowering barriers for the development of biological weapons.** The ability to rapidly modify a genome at relatively low cost compared to previous methods could make CRISPR systems attractive for nefarious actors at all levels, from individuals through nation states. **In the realm of biosecurity threats, CRISPR may be misused to create increased-virulence pathogens, neurotoxins, and even de novo organisms (DiEuliis, Berger, and Gronvall 2017; DiEuliis and Giordano 2017). A de novo organism would be completely synthetic, although it may have the same genome as an existing pathogen like smallpox.** Creating a completely novel organism using synthesis is theoretically possible, but it is likely to require extensive training, funding, and time for research and development, which is less possible for some types of actors (Gibson et al. 2010). **A recent National Academies of Sciences, Engineering, and Medicine study, Biodefense in the Age of Synthetic Biology (2018), was undertaken to develop guidance on evaluating biosecurity risks associated with new biotechnology.** The authors categorized potential threats by level of concern and offered potential solutions or safety measures that could reduce the risk of a certain technology. **The authors recommend that the US Department of Defense, who requested this study, continue to innovate and engage in biotechnology, but that an assessment framework should also be used to examine novel biotechnology and its potential broader applications in the scientific and public spheres.** The authors also categorized potential risks by relative concern, identifying the re-creation of known pathogens, such as smallpox, as among the highest of concern, while rating the creation of a novel pathogen as a lower risk. CRISPR could allow for rapid, efficient editing of a pathogen to possess the virulence factors of another pathogen, or it could allow a researcher to recreate a known pathogen whose genome is published. **Given these biotechnology areas of concern, the misuse of CRISPR warrants recognition as a potential biosecurity threat.**

The gene drive technology that promises benefits to health and agriculture could also be engineered to create devastation for crops or directly used against human populations. The technology can be very unpredictable and this poses a wide array of threats to the United States.

> **Scudellari**, Megan (freelance science writer and journalist based in Durham, North Carolina**,** specializing in the life and environmental sciences). "Self-Destructing Mosquitoes and Sterilized Rodents: the Promise of Gene Drives." ***Nature News***, Nature Publishing Group, **9 July 2019**, www.nature.com/articles/d41586-019-02087-5.

Another concern is that gene drives have the potential to alter entire populations and therefore entire ecosystems. They could also, in theory, negatively affect human health by causing the malaria parasite to evolve to be more virulent or to be carried by another host, says molecular biologist and bioethicist Natalie Kofler. She is the founding director of the Editing Nature group at Yale University in New Haven, Connecticut, which aims to address environmental genetic technologies worldwide. "**This technology has the potential to be immensely powerful and to change the course of things that we may not be able to predict,"** says Kofler.

Another threat the U.S. faces is biotech espionage from competing nations like China. While this type of threat may not result in an attack, it could harm the United States in economic ways. These threats are uniquely difficult to prevent since eliminating the threat could also remove opportunities for collaboration and innovation.

Moore, Scott (political scientist and administrator at the University of Pennsylvania). "In Biotech, the Industry of the Future, the U.S. Is Way Ahead of China." ***Lawfare***, 17 Feb. **2021**, www.lawfareblog.com/biotech-industry-future-us-way-ahead-china.

The U.S. biotechnology sector also faces other threats, not least growing espionage and intellectual property theft by foreign actors, especially those linked to China. Several high-profile cases brought by the U.S. Department of Justice's China Initiative have involved biotechnology researchers, and American biotech firms have been top targets for cyber theft and intrusion. Sustained outreach to researchers and research institutions is critical to preventing such theft. **But efforts to clamp down on the threats posed by espionage and intellectual property theft can easily go too far and must preserve the researcher mobility and data-sharing that is essential to doing cutting-edge science.**

Therefore, it may be critical that the international community act in multiple ways to address this threat. One way to address these threats is through the development of a framework for the use of biotechnology.

Dieuliis, Diane (Sr. Research fellow at National Defense University), and James **Giordano** (Prof. of Neurology and Biochemistry, and Chief of the Neuroethics Studies Program of the Pellegrino Center for Clinical Bioethics at Georgetown University). "Gene Editing Using CRISPR/Cas9: Implications for Dual-Use and Biosecurity." ***Protein & Cell***, vol. 9, no. 3, **2017**, pp. 239–240., doi:10.1007/s13238-017-0493-4.

We propose that **agreed-upon international, ethical "norms" for human modification for therapeutic purposes are relevant and applicable to any such use of this technique. Kang et al (2017)** advocate international standards of ethics, and note efforts made to date by the National Academies (2017) in this regard. **We concur with the need for**

international ethical standards and guidelines, and also note the need for more engaged discourse to define the needs, values and ethical system(s) and principles to be employed (Palchik, Chen, and Giordano, 2017; Lanzilao, Shook, Benedikter, and Giordano, 2013) Furthermore, in recognition of the potential risk/threat posed by genetic modification, we strongly endorse involvement of the Biological Toxins and Weapons Convention (BTWC), in order to ensure inclusion of biosafety and biosecurity communities in any such deliberation and determination of standards. **Templates may exist and could be consulted for the development of international norms and best practices through engagement of expertise in technical aspects of emergent technology and security fields (Talinn Manual, NATO, Carnegie Endowment 2017). Expanding the scope and platform of international dialogue can be instrumental to ensuring that all aspects of emerging biotechnological tools and methods are evaluated for their potential to be weaponized or used in other ways that threaten public safety (Gerstein and Giordano, 2017).**

Another route for dealing with biotech threats is the development of countermeasures. For example, DARPA is currently involved in developing gene drives to counter possible damaging ones that could be released into crops and animal populations.

West, Rachel M., and Gigi Kwik **Gronvall**. "CRISPR Cautions: Biosecurity Implications of Gene Editing." ***Perspectives in Biology and Medicine***, vol. 63, no. 1, **2020**, pp. 73–92., doi:10.1353/pbm.2020.0006.

Attempts to use gene drives to decimate crops or impact local resources could present a biosecurity threat that could have a wide range of consequences. Keeping this in mind, the Defense Advanced Research Products Agency **(DARPA) created the Safe Genes Project to not only address potential issues in gene drive technology and biosecurity, but to also promote defensive research to create countermeasures** (DARPA 2017). Seven research teams are funded by the project, with each having an overall goal of (1) developing genetic tools to provide better control of gene drives; (2) creating drug-based treatments to reverse or prevent effects of gene drives; or (3) identifying ways to mediate gene drive impacts on ecosystems. **This cooperative effort between government and scientists is an excellent example of forward-thinking research that helps support gene drive research by making it safer and more responsible.**

Also, the United States could develop better export controls to manage the materials transported to other countries that might be used for bioweapons.

Moore, Scott. "In Biotech, the Industry of the Future, the U.S. Is Way Ahead of China." ***Lawfare***, 17 Feb. **2021**, www.lawfareblog.com/biotech-industry-future-us-way-ahead-china.

Beyond its shores, t**he United States should work with its partners and allies to enhance export controls on dual-use biotechnology—used for both peaceful and military**

gain—especially DNA templates. Many forms of genetic material and synthetic biology products are already subject to U.S. export controls, but gaps remain, and screening for genetic sequence orders relies primarily on voluntary regulation by biotech firms. **Better coordinating export controls among major economies and U.S. allies can dramatically reduce the risk of sophisticated bioweapons development in the decades to come. When it comes to biotechnology, the industry of the future, the U.S. remains well ahead of its rivals, including China.** That's something Americans can, and should, take pride in. **But the U.S. must make proactive investments and undertake significant reforms now to ensure that things stay that way.**

Indeed, there is a growing consensus that emerging technologies like gene editing must be a part of the National Defense Strategy and it should include international institutions.

Sherman, Justin (nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative. He is also an op-ed contributor at *WIRED* and researches at the Tech, Law, & Security Program at American University Washington College of Law and at *Lawfare*'s Trustworthy Hardware and Software Working Group) and Evanna **Hu**. "How the next National Defense Strategy Can Get Serious about Emerging Technologies." ***Atlantic Council***, 19 Feb. **2021**, www.atlanticcouncil.org/blogs/new-atlanticist/how-the-next-national-defense-strategy-can-get-serious-about-emerging-technologies/.

The next NDS should include sophisticated, nuanced strategies for emerging technologies based on the maturity of the technologies along a spectrum. It should feature distinct strategies for already-emergent technologies such as AI, and for emerging technologies such as CRISPR gene editing and quantum computing. It should take an inclusive approach that integrates the perspectives of the commercial sector and civil society from the start, as opposed to the government outlining strategies and values before engaging with other sectors. And **it should involve collaboration with international institutions on standards, ethics, and frameworks to ensure that US values governing these technologies align with the values of democracy and the international community, and that US technological capabilities are interoperable with those of its partners and allies.**

This leads to the question of what international institution would be best equipped to deal with the challenges of emerging biotechnology. One possibility is the North Atlantic Treaty Organization. As their 2018 "Framework for Future Alliance Operations" suggests, they are keenly aware of the threats posed by emerging technologies.

NATO. "Framework for Future Alliance Operations." ***North Atlantic Treaty Organization***, **2018,** https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf

> **The future will likely bring a wide range of new threats coming from emerging technology** or from new, creative, and innovative tactics, techniques, procedures, capabilities, or doctrine. Without incurring the cost of research and development, hostile actors can capitalise on technological advancements and translate them into capabilities that threaten the Alliance. **Examples of areas where technology could revolutionise warfare** are sub-surface and subterranean operations, swarm techniques, space based weapons, directed energy, autonomous systems and sensors, quantum computing, unmanned systems, electromagnetically launched projectiles, renewable energy, **artificial intelligence,** additive manufacturing/3D printing, **biotechnology** and nanotechnology. **Forces must be able to identify, monitor and understand these new threats, and develop protective measures.**

NATO as a security organization might be in the best position to partner with the United States on the security threats presented by emerging technologies. They are in many ways uniquely situated to help negotiate the limits of the technologies and simultaneously initiate the cooperation needed to stay on the cutting edge needed for leadership and security.

> **Murray**, Rob. "Building a Resilient Innovation Pipeline for the Alliance." ***NATO Review,*** 1 Sept. **2020**, www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/index.html.
>
> Today, **NATO's competition is a global one and the race is one of technological adoption – that is, the acceptance, integration and use of new technology in society. From artificial intelligence to quantum and everything in between, governments are in a race to leverage these technologies at scale and speed – first adopter advantage for emerging disruptive tech could not be more prevalent in the world of geopolitics and deterrence**. Indeed, **the nations that win this race may be those with the most agile bureaucracy rather those with the best technology. In contrast to the Cold War, the United States and its NATO Allies are unlikely to simply outspend others.** In a post-Covid-19 world, rebalancing public finances could see f**urther financial pressure placed on Allied defence budgets. We now need a different advantage, one which will deliver in the short term and build resilience over the longer term – more defence at less cost with least delay. This starts with our people, their creativity, education and access to funding. It ends with a robust pipeline of new dual-use (civil and military) technologies constantly being created, commercialised and capitalised upon. The Alliance's transatlantic nature places it in a unique position within the international order to provide both demand-side policies and supply-side resources that can genuinely build such a pipeline, creating not only innovations but entirely new markets** – as Eisenhower noted: the foundation of military strength is economic strength. Recent history would suggest, the model of democracy and Allied governments' willingness to make big bets on mission-oriented technology does indeed create new markets and it is this model, underpinned by shared values, which will be key to NATO's longer term success.

With the US, NATO could play a vital role in reacting to biological threats in the future. As the Coronavirus pandemic has shown, biological threats found in nature are just as likely to decimate countries as man-made pathogens. There is clearly a need for more international cooperation and alignment in dealing with biological threats and this could be achieved through a US-NATO partnership in the area of vaccines.

> **Paun**, Carmen (writer, ***Politico***), and Ryan **Heath** (Sr. editor, ***Politico***). "How the Coronavirus Can Prepare Us for Bioterrorism." ***POLITICO***, 24 July **2020**, www.politico.com/news/2020/07/24/how-to-prepare-for-bioterrorism-courtesy-of-coronavirus-380689.
>
> **Whether it comes from natural causes or from an enemy, the crippling effects of a new virus are the same**, said Stefano Stefanini, a former Italian ambassador to NATO, now head of the Brussels office of Project Associates, a consultancy. Stefanini thinks **NATO should have reacted to coronavirus in the same way it would react to a biological attack,** he said. **In the future, the defense alliance should consider how to help its members better prepare for this kind of emergencies, maybe as part of their defense spending budget**, he said. **When a vaccine would be approved, NATO could play a significant role by using its logistics to help deploy it to member countries and maybe to other countries,** as well, Stefanini said. NATO Spokeswoman Oana Lungescu rejected this criticism, saying the organization is not the first responder in these situations. That's up to nations, but **NATO can use its capabilities to support them**, she said.

Vaccine diplomacy from the US has lagged, so far during the pandemic, but a new NATO partnership could invigorate US soft power and leadership.

> **Prasad**, Kislaya (research professor at Smith School and a guest scholar at the Brookings Institution). "Unless the U.S. changes its vaccine policy, the world will look at us like hoarders." ***Fortune.com*** 4/4/**2021**
>
> **But even if one were to discount the importance of soft-power diplomacy, the Western response is incomprehensible for at least three reasons. First, the hoarding of vaccines does not help the West fight COVID-19**. So long as the pandemic continues to rage around the world, new coronavirus variants resistant to existing vaccines are likely to arise and spread globally. **Second, vaccine nationalism has adverse economic effects**. In an interconnected global economy, if large parts of the world remain devastated by the pandemic, the impacts are felt elsewhere. **Finally, the pandemic has elevated global public perceptions of the Chinese and Indian pharmaceutical sectors' capabilities, possibly at the expense of U.S. pharma companies.** Moreover, less-developed countries now know that in the event of another global health crisis, they are essentially on their own, and need to invest in domestic capabilities. **U.S. leadership during past global crises has cemented its standing and influence in the world, and furthered its geopolitical and economic interests. It is past time for the**

U.S. to do the same in its vaccine diplomacy. Vaccinating the world's population must become an American priority.

Negative Ground

While it is easy to imagine a catastrophic event involving biological weapons, it is much more difficult to actualize that event. While affirmative teams will have the ability to describe the magnitude of potential impacts from biological attacks they are also under the burden to prove their probable use which will be a greater challenge. This will help level the playing field for the negative team.

Vogel, Kathleen M. (associate professor in the School of Public Policy, University of Maryland, College Park, and a Senior Fellow at CISSM), **and** Sonia Ben **Ouagrham-Gormley** (George Mason University GMU, Dept of Public and Internat'l Affairs). "Anticipating Emerging Biotechnology Threats: A Case Study of CRISPR." **Politics and the Life Sciences**, vol. 37, no. 2, **2018**, pp. 203–219., doi:10.1017/pls.2018.21.

With all of the foregoing said, however, let us assume that one is able to reliably and accurately mutate a pathogen using CRISPR or one of its gene-editing variants. **This does not mean that one automatically has a biological weapon**. **Creating a mass-casualty biological weapon requires more than mere access to a pathogen, a particular technique, or a piece of biotech equipment** — although all of these are important components. To create a potent bioweapons capability, there are a variety of technical issues that must be addressed. First, one must acquire access to a virulent pathogen or toxin — **CRISPR may allow one to create a lethal, or more lethal, variant of a pathogen or toxin, but this is not without problems.** As noted earlier, the Soviet Union learned the hard way that even though they created a highly antibiotic-resistant strain of tularemia bacteria, it was so environmentally sensitive that it could not survive in the environment. Therefore, **merely being able to genetically engineer a pathogen did not ensure a viable bioweapons capability. Also, one still has to overcome other hurdles. Unless one creates a highly infectious agent, a would-be terrorist would have to determine how to produce larger quantities of the agent**. Production in larger batches is not as trivial as growth of an agent in a petri dish. The former Soviet Union experienced difficulties in scaling up its bioweapons agents in new facilities. Along with production, one also has to think about how to protect the agents to survive in the environment, as **many biological agents and toxins can be environmentally sensitive.** The processing of agents is a key challenge in developing a bioweapons capability — the United States, Russia, and Iraq all encountered problems in creating special formulations to stabilize their bioweapons agents. One then has to find an appropriate delivery form of the material (e.g., liquid or dry), which can also pose challenges for viability, and then employ an appropriate delivery device under the right conditions. Former U.S. bioweaponeer Bill Patrick has noted, **"You can have the best agent in the world, but the physics of dissemination mean that unless you have good conditions and with a good delivery system to get that *improved* agent on target, you're going to fail."** Past state and nonstate bioweapons programs have shown that addressing these factors requires knowledge, specialized skills, and management and organizational expertise, as well as materials, infrastructure, and equipment. Therefore, the important takeaway here is that gene editing is only

one small component of an entire process required to produce lethal biological weapons. **Unless gene editing (or other science and technology developments) can be shown empirically to alter the other factors of bioweapons development, technical hurdles will remain.** This also points to the need to look not only at gene manipulation but also at all of the other factors shaping production, processing, and delivery of bioweapons agents in threat assessments.

Also, the regulation of biotechnology could have unforeseen impacts on innovation and economic development. Groups that invest in emerging technologies in the biotech industry may see a foreign policy aimed at controlling biotech use as hostile to free market capitalism.

National Venture Capital Association. "Emerging Technology Definition Must Protect American Innovation." ***States News Service,*** 11 Jan. **2019**. *Gale Academic OneFile Select*, link.gale.com/apps/doc/A569194284/EAIM?u=ksstate_wichita&sid=EAIM&xid=fa626305.

The National Venture Capital Association (NVCA) recently made formal recommendations in the Commerce Department's rulemaking process to define so-called "emerging technologies" that will be subject to export controls. These newly defined emerging technologies will also feed directly into the Foreign Investment Risk Review Modernization Act (FIRRMA) process, and certain investments into these types of companies may trigger a CFIUS filing. **In announcing the comment period, Commerce asked for feedback on 14 categories that includes AI/machine learning, 3D printing, biotechnology, and several other technology areas that are major focuses of U.S. startups and venture investment.** "**American innovation could be seriously hampered unless the Commerce Department acts with precision in classifying emerging technologies**," said Bobby Franklin, President and CEO of NVCA. "A targeted approach is needed in this rulemaking. By categorizing only those technologies that have significant defense uses and not those that merely have broad commercial implications or incidental national security significance as emerging technologies, the government can ensure the impact on American scientific and technological advancement is minimized while still protecting important national security interests." In its submission, NVCA emphasizes three key points: (1) Venture capital is the single largest driver of emerging U.S. company innovation and draws on capital and talent from across the world. **An overbroad definition of emerging technologies** (thus an overbroad application of FIRRMA) **may have devastating consequences for the innovation economy**. (2) Many of the representative general categories of technologies listed in the request for comments are not yet well-defined. Because technologies that could be deemed to fall into those categories are widely used across many emerging technology companies, a broad set of controls could sweep in many unintended target companies and technologies. (3) The case for investing in many U.S. emerging technology companies relies in many circumstances on their ability to find talent and worldwide commercial markets for their innovative products. **To the extent that the new rules prevent U.S. companies from accessing that talent and those markets, global venture capital may well redirect to innovators in other nations.** In addition to NVCA's comments to the Commerce Department, it has also provided input to the Treasury Department about its pilot program under FIRRMA. On November 7, NVCA filed comments that asked for clarification in ten areas that have caused unneeded confusions for venture capitalists and high-growth startups.

The last four years of America First has made many countries wary of relying on the United States. While Biden may be ready to initiate conversations around partnership that does not mean our allies will so easily fall back in line. For example, France's president signaled Europe must build its own defense capabilities to avoid its security dependence on the US:

> **Sanger,** David E. (Adjunct Lecturer in Public Policy, is the Chief Washington Correspondent of ***The New York Times***). **, et al**. "Biden Tells Allies 'America Is Back,' but Macron and Merkel Push Back." ***The New York Times,*** 20 Feb. **2021**, www.nytimes.com/2021/02/19/us/politics/biden-munich-conference.html.
>
> But **Mr. Macron**, speaking in English to answer a question, also **argued that Europe could not count on the United States as much as it had in past decades**. "We must take more of the burden of our own protection," he said. In practice, it will take many years for Europe to build up a defense arm that would make it more self-reliant. But Mr. Macron is determined to start now, **just as he is determined to increase the European Union's technological capacities so that it can become less dependent on American and Chinese supply chains. Mr. Biden, in contrast, wants to deepen those supply chains — of both hardware and software — among like-minded Western allies in an effort to lessen Chinese influence. He is preparing to propose a new joint project for European and American technology companies** in areas like semiconductors and the kinds of software that Russia exploited in the SolarWinds hacking.

If anything, the last four years taught our partners they must be ready for anything come 2024 and if that is a second term for Trump or Trump 2.0, a U.S. partnership may not be worth the paper it is printed on.

In addition, there are ample avenues outside of a NATO partnership for negative teams to access benefits. The U.S. could partner with the World Health Organization, the United Nations, The International Monetary Fund, or any international organization to support or regulate biotech development or use. Also, the negative team could propose a bilateral partnership with an individual country to form a biotech alliance. This would provide a clear contrast to the affirmative team while still accessing advantages from the resolution.

Negative teams could argue that there are substantial disadvantages to cooperating with NATO on biotechnology. One disadvantage would be the potential backlash from countries like

China and Russia. While the policy would certainly be designed to contain these two countries, it could create a more dangerous situation if China and/or Russia view the policy as aimed directly at them. This may result in an escalation of tensions between the West and Russia and/or China. These countries are currently cooperating on a Space Program. What if the U.S. cooperation with NATO on biotechnology solidifies these two powerful countries together on another technological front? China is also still aggressively seeking control of the South China Sea. Will this policy make it more difficult for the US to address issues with China on other matters like the South China Sea dispute?

Cybersecurity

Affirmative Ground

The complexity of computer networks and the difficulty of preventing, detecting, responding to, and recovering from a cyber-attack make it nearly impossible for any single country to develop an effective unilateral approach to cybersecurity. While the U.S. has long been a global leader in cybersecurity, a decades' long policy focusing on Offensive Cyber Operations (OCO's) through covert NSA acquisitions as a national policy, as opposed to a comprehensive national security policy focused on defensive cyber security, left our government and businesses' cyber networks vulnerable to exploitation by private hackers, transnational criminal organizations, and those supported by national governments. Post-Trump, the hacking and release of CIA hacking tools by Wikileaks eliminated any offensive advantage of U.S. government hackers and left the Biden Administration scrambling to create new digital security solutions.

> **Riley**, Tonya."The Cybersecurity 202: NSA director says intelligence has a big[PM1] blind spot: domestic Internet activity." ***Washington Post,*** 3-26-2021. https://www.washingtonpost.com/politics/2021/03/26/cybersecurity-202-nsa-director-

says-intelligence-has-big-blind-spot-domestic-internet-activity/#click=https://t.co/kg8XkfRoXH

> A judge rejected a request by an ex-CIA employee to dismiss charges of leaking hacking tools. **A judge denied former CIA employee Joshua Schulte's bid to dismiss espionage charges** on the grounds that the grand jury that indicted him did not have enough Hispanic or Black individuals, Larry Neumeister of the Associated Press reports. **A trial for Schulte, who is accused of leaking CIA hacking tools to WikiLeaks and has pleaded not guilty to all charges, is expected to begin in October after a jury deadlocked last year. WikiLeaks' 2017 release of the hacking tools was one of the most significant leaks in the CIA's decades-long history and laid bare the agency's hacking and surveillance methods. The Biden administration is readying an executive order to require companies to disclose breaches to U.S. government clients. A draft version of the order would also require companies to keep more records for investigations of the breaches and work with federal agencies as they respond,** according to Reuters's Christopher Bing, Nandita Bose and Joseph Menn. The order could be made public as early as next week, they write. **The executive order comes as the Biden administration plans its responses to the devastating SolarWinds and Microsoft Exchange hacks.** A National Security Council spokeswoman told Reuters **no decision has been made on the final content of the executive order.** Anne Neuberger, the deputy national security adviser for cyber and emerging technology, previewed the executive order earlier this month, when the government was still primarily grappling with SolarWinds. Neuberger said at the time that t**he executive order would "focus on building in standards for software, particularly software that's used in critical areas."**

Additionally, the U.S. is confronting a more pressing challenge regarding the SolarWinds hack of the Microsoft Exchange servers, and the recent cyber-attack on our energy infrastructure, Colonial Pipeline. Our adversaries are using our own weapons against us. Unfortunately, the U.S. did not catch this attack, and a global cyber-security firm alerted the world to the attack.

The Advanced Persistent Threats (APT) to global computer networks left vulnerable the most critical infrastructure systems: supply chains, providing the public with everyday goods and resources, electrical grid systems, medical facilities, global financial systems, and command and control (C2) weapons systems, the backbone of militaries across the world. APT's are typically carried out by individuals with ties to or working directly with nation states, although attribution remains problematic.

A failure of the U.S. to act in response to these threats could indicate the danger of falling woefully behind other developed nations in the areas of technology and emerging threats facing

the world. The fear of failure is driving the Biden administration to draft aggressive executive actions to confront the challenges, and to propose significant funding increases for the U.S. Cybersecurity and Infrastructure Agency (CISA), decimated by the previous administration and John Bolton, NSA advisor. Biden spoke directly to the involvement of the Russian government. Senate members, including ranking Democrats, echo Biden's call for action, and indicate Russia must bear the consequences of their cyber belligerence, and the global community must establish better rules of conduct and consequences in cyberspace. It is crucial the American public understand this growing threat, so they will support political changes needed to protect our country.

Because the threats are not unique to the U.S., and because our government does not have the ability to resolve cybersecurity threats without cooperation from allies and members of the global community, international actions are warranted and required. NATO is stepping up to take the lead to create global solutions to protect all citizens across the globe. Since 2016, NATO has taken steps to create frameworks for its members to prevent global conflict and resolve cyber threats from both state and non-state actors. NATO is committed to examining the specific challenges brought by cyber threats. The cooperative framework that exists within NATO provides the international community with the tools and resources to address cyber threats. Individual states, alone, cannot resolve this global challenge.

> **NATO**. "Joint press conference by NATO Secretary General Jens Stoltenberg with the EU High Representative for Foreign Affairs, Federica Mogherini." ***NATO,*** 12-6-2016. https://www.nato.int/cps/en/natohq/opinions_138729.htm
>
> Good afternoon. We have just finished a meeting where we addressed the cooperation between NATO and the EU. And the meeting was attended by High Representative / Vice President Federica Mogherini and with the Minister from Sweden and the Ambassador of Finland, so in addition to the 28 members of the Alliance and Montenegro, we also had representatives of the European Union present at the meeting. And it's always a good pleasure to welcome you to NATO, Federica, especially when we are able to agree on such a substantial list of measures to take our cooperation forward. And **we have been working together on how to strengthen and how to enhance the cooperation between NATO and EU for a long time, so therefore I think today we really mark a milestone in our**

efforts to build our cooperation and to strengthen the partnership between NATO and the EU. The security of Europe and North America is interconnected. **A stronger NATO is good for the EU and a stronger EU is good for NATO. And strengthening our strategic partnership is more important than ever.** First, **we all face new threats and new security challenges, which combine military and non-military means of aggression. Such as hybrid, cyber, terrorism. And neither NATO nor the EU has the full range of tools to respond to these challenges, so therefore we have to cooperate.** Second, the EU is taking steps in strengthening European defence, which we welcome. It is important that these steps are complementary with NATO efforts. And third, the strength of the transatlantic bond is vital to our security. **Strong ties between NATO and the EU bring North America and Europe closer together.** In Warsaw in July, I signed a Joint Declaration with Presidents Tusk and Juncker. We said at the time that we had never done so much together. Now we are going to do even more together. We have identified over forty proposals in several key areas. They are pragmatic, but they are ambitious. **On hybrid, we agreed on concrete measures to increase situational awareness. And to bolster our nations' resilience.** On maritime, we enhanced cooperation between Operations Sea Guardian and Sophia in the Mediterranean. Through logistical support and information sharing. **On cyber, we will strengthen our mutual participation in exercises, and foster research. NATO and the EU will also work more closely together to build the capacities of our partners.**

Through the development of effective policies to create new cyber defenses and an internationally agreed upon framework for conduct and conflict in cyberspace, the NATO actor, in this resolution, creates a discussion of advantage areas that give affirmative teams a diversity of options to debate. Intrinsic to this topic will be discussions of the changing relationship of the global superpowers, as well as nations whose extensive cyber capabilities create new power dynamics in a globalized world. The relationships between the U.S., Russia, China, and the EU are central to this topic and allow the affirmative to look at specific avenues to create cooperation between actors and help build on global efforts to deter conflict.

Stoltenberg, Jens (NATO Sec. General). "NATO and Cyber: Time to Raise our Game." ***Defense News***, 7-28-2016, https://www.defensenews.com/smr/road-to-warsaw/2016/07/08/nato-and-cyber-time-to-raise-our-game/

We may not see it but, in the realm of cyberspace, our countries are under attack every single day. A few years ago it was cyber-attacks on financial institutions that made the headlines. Today, it is attacks on critical networks and infrastructures – disrupting services and, in some cases, bringing modern life to a grinding halt. In fact, **what was once a nuisance has become a strategic challenge. Two years ago, a cyber-attack temporarily blocked access to NATO headquarters' website. Recently, a series of cyber-attacks was launched against German state computer systems, including to gather intelligence on critical infrastructure such as power plants. And in Ukraine, cyber-attacks have been used as a weapon of so-called "hybrid" warfare. States and non-state actors are increasingly**

using cyber-attacks to achieve their diplomatic and military objectives. So two years ago, **NATO allies acknowledged that the impact of cyber-attacks could be as harmful to our societies as a conventional attack and made clear that cyber defense is part of the alliance's core task of collective defense. Cyber-attacks can also seriously undermine NATO's missions around the world. Our forces are increasingly likely to operate in environments where adversaries use cyber-tools to disrupt our decision-making. To ensure that NATO can do its job of protecting its citizens and territory against any threats, we have to be just as effective in the cyber domain as we already are on land, in the air and at sea.**

At the heart of this discussion is the crucial issues of evolving power dynamics as the world transitions from a post-cold-war alignment to a world of emerging powers whose fates seemed destined for conflict. The affirmative can access an ever-growing body of literature that explores cooperation in this new multilateral world, and the manner in which the U.S. and other actors should engage with each other as alliances transition and shift with the reality of a changing world. NATO is a defensive alliance committed to its mission of protecting its member nations' citizens and their territory. NATO is the appropriate actor because of its commitment to strict adherence to international law. NATO's values ensure the coalition is best suited to create a peaceful cyberspace world in the future.

Stoltenberg, Jens**.** "NATO and Cyber: Time to Raise our Game." ***Defense News***, 7-28-2016. https://www.defensenews.com/smr/road-to-warsaw/2016/07/08/nato-and-cyber-time-to-raise-our-game/

For all that NATO is doing to adapt to a changing world, one thing will never change: we are a defensive alliance, whose mission is to protect NATO's citizens and territory, and whose actions will always be proportionate and in strict accordance with international law. That, in turn, means that we strongly support efforts to foster a more transparent and secure cyberspace, through the development of voluntary norms of behavior by individual states and related confidence-building measures. NATO is founded on the shared values of liberty, democracy, human rights and the rule of law. That is why we are determined to ensure that cyberspace remains the place for peaceful, open communication and debate that we all need it to be.

Within this discussion, affirmatives have the ability to take theoretical positions to support the resolution to create strong debates, including the role of U.S. hegemony in a post-

Trump global world, the role of the NATO alliance in the modern world, the effectiveness of deterrence in cyberspace, and the effectiveness of offensive versus defensive cyber policies. Within the broader discussion of NATO and geopolitics that this resolution brings, is the manner in which our global economy functions interdependently, and the vulnerabilities of multiple industries to cyber-attacks threatening the safety and security of populations across the world. At the heart of this topic, the affirmative has access to explore the specific effects of cyber-attacks on key areas of the global economy including: banking and finance, health care, energy security, transportation infrastructure (ports and shipping), military and defense, aerospace, and the emerging technology industry. Regardless of enemy provocations, NATO is the appropriate leader in cyber defense because it is committed to creating peaceful outcomes with adversaries by avoiding conflict. NATO has the ability to create the environment for dialogue though the creation of credible cyber deterrence.

> **Stoltenberg**, Jens. "Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers." ***NATO***, 2-16-2017. https://www.nato.int/cps/en/natohq/opinions_141340.htm
> **JENS STOLTENBERG (NATO Secretary General): We will continue to work for dialogue with Russia. We don't want to isolate Russia, we don't want a new cold war, we are working for a more constructive relationship with Russia and we will continue to do exactly that. But of course our dialogue with Russia has to be based on some core principles, the respect for the territorial integrity of all nations**, states in Europe including Ukraine **and of course we have to combine dialogue with credible deterrence.** And that is a lesson we learned actually during the Cold War and a lesson which taught us that **it's possible to have dialogue but at the same time have a firm, predictable approach including credible deterrence.** This worked towards the Soviet Union during the Cold War and I'm absolutely certain that **this strategy is also the right strategy in approaching Russia in a very different security environment today. So we will continue to deliver credible deterrence, be firm and predictable; but at the same time strive for a more constructive relationship with Russia.**

Negative Ground

While at first glance, this topic may look daunting for the negative; a closer examination allows teams a diverse set of strategy options encompassing both policy and kritikal

argumentation. Regardless of stylistic norms within all debate circuits, this resolution will allow students, at all levels, the ability to easily access both literature and arguments for this resolution. As the community moves towards "case lists" for novices, the unique nature of this resolution for case areas allows students to develop a broad range of debate skills and knowledge making them life-long learners.

The harm areas create broad emphasis for case debate at almost all levels. The impact areas allow both offensive and defensive arguments to be researched and advocated by the negative as part of a broader in-round strategy. More importantly, there should be a strong set of arguments as to the ability of NATO to resolve the specific cyber threats involving the U.S. A robust case debate engaging both the harms' areas and solvency can be accessed and made by teams. In addition, a discussion of the Biden administration and the U.S. government's ongoing response to cyber threats can be argued. A powerful literature base exists to support arguments related to the effectiveness of the U.S.'s current cyber strategy.

Because of the diversity of harms areas, the negative gains access to a various set of case specific disadvantage links related to arguments concerning the foreign relations and the outcome of policy changes, the effect of these policies on specific industries and the economy, and arguments relating to the political nature of the changes affirmatives will be discussing. There is a significant assortment of case specific disadvantages, as well as politics arguments.

In addition to the disadvantage ground, negatives have a range of counterplan options with these topics, all supported by robust literature. Affirmatives must carefully choose their solvency evidence as literature supports a number of negative counterplan approaches testing the efficacy of the affirmatives plan. Key negative ground will include a discussion of which actor

is right to resolve the central concerns being discussed. Negatives can retrieve evidence to support arguments of the U.S., as a solitary actor, would be better suited to solve the harms. Other international organizations are better equipped, through their membership and structure, to resolve the concerns, or that public/private partnerships involving non-state actors (technology companies and business) and government would be most appropriate. Probably the States CP, for this topic, is not an option. For the kritik debater, access to the literature examining the underlying epistemological and ontological realities, will be an asset to debating the topic. The authors believe of the importance that teams have access to specific links to a diverse set of kritikal argumentation lending itself to check the breadth of affirmative argumentation. Kritikal teams should have ingress to links to critical arguments including: Anti-Blackness, Queer Theory, Bio-power, Capitalism, International Relations Theory and Security Studies, Post Modernism, Communication Theory, and Surveillance.

As the consequences of the recent Solar Winds hack become more apparent, the private and government sectors of the world are faced with creating an effective cyber strategy to combat looming challenges involving hybrid warfare. In the 21st century, it becomes crucial to consider the most effective global actors who can resolve the issue of these emerging threats. While the United States' role in this pressing crisis is debatable, what is not in question is the need of the international community to collaborate in creating solutions suitable to the complex cyberspace environment. As the U.S. and Russia continue playing a cat and mouse diplomacy game, Putin tries to adjust to the Biden administration's sanctions related to cyber-attacks. However, NATO continues to press forward to coordinate and build a global cybersecurity framework to protect private and public sectors from the dangers of the ongoing low-intensity cyber war being fought on our global networks every day.

VII. Quality

In President Biden's 100-day address, he articulates "crisis and opportunity," or as Sir Winston Churchill is noted to claim, "Never let a good opportunity go to waste." Now, with the recent ongoing NATO deliberations regarding AI, human gene editing, and Colonial Pipeline and SolarWinds attacks, the U.S. must take these crises and seize the opportunity to forge a multilateral approach to these threats. In this address, Biden's focus is primarily domestic. However, the U.S. is facing daunting threats from Russia, China, and others on multiple fronts. This topic will continue to be highly discussed with a steady stream of new relevant research. In an increasingly untenable global world, the next crisis will be like no other with the use of emerging technologies on the battlefield. This topic will encourage discussions of international relations, the STEM field, and the role of international organizations in foreign policy. Each of these areas is vital to an increasingly technology-driven, globalized world. Therefore, it is imperative that debaters interact with issues centered around both technology and international policy. Due to the breadth and depth of the concerns outlined in this paper, the authors feel assured that debates will not become stale. Rather, the argumentation will grow increasingly nuanced as the season progresses.

VIII. Material

Recent topic selection meetings have made it clear that equity in resources and opportunity are both important considerations for our coaches and community. Through the collection of research and the discussion of this topic, these authors believe there is a plethora of material discussing emerging technologies, as well as the threats and opportunities they pose to the world. Access to topical, relevant, and contemporary commentary and analysis of artificial intelligence, bio-technology, and cybersecurity is easily attainable for all debaters. The focus on

NATO and U.S. government policies creates a set of research without the need for expensive academic databases. As the world responds to the real threats and opportunities of emerging technologies, both U.S. and global experts are weighing in daily creating an enormous database of evidence.

These authors are confident this topic will enable students to access quality research and analysis by global experts, which allows them to cross over into multiple disciplines and curricula creating life-long learners. Students in Urban Debate Leagues, rural, and small school communities, as well as the "National Circuit," can debate at all levels. Students will be able to engage in discussion of international relations from a perspective other than the U.S.; the topic allows students to explore the latest trends in science and technology, information that is often not found in other classes. Debates on this topic will not be limited to certain policy perspectives, but should allow and foster properly scaffolded skills' development to enhance argumentation. While we feel that the topic is broad, the strength in it is the balance of affirmative and negative material.

An exploration of kritikal literature expands well beyond security studies and International Relations (IR) Theory. Students will have the opportunity to work with coaches to explore multiple genres of kritikal literature including Critical Race Studies, Queer Theory, Colonialism, Post-modernism, Communication Theories, and Economics. Thanks to the expanded availability of free access to online academic research, and through the efforts of file sharing, debaters can find many alternative perspectives.

IX. Balance

This topic proposal was crafted with meticulous attention to the need for a robust exchange of ideas. The topic of emerging technologies generally, and the resolutions the authors

have proposed specifically, do not inherently advantage either the affirmative or the negative. As outlined in this paper, there is an ample research base for both sides to create their arguments – from the utility of NATO or another entity as the agent of action; to the specific use cases of artificial intelligence, biotechnology, and cybersecurity technologies; to a vast range of advantages and disadvantages in light of the important international affairs, security, economic, and scientific-technological issues implicated in this topic.

To be sure, each of the emerging technologies mentioned in the proposed resolutions involve complex issues of public policy, technological development, and global security. Debaters will come away from this experience with a well-rounded understanding of how these technologies are reshaping society, the advantages and disadvantages of different policy approaches to addressing the challenges and seizing the opportunities these technologies present, and how the issues surrounding emerging technologies will shape the global security agenda for decades to come. Students will gain knowledge of how crisis and opportunity must be met with a collaborative approach to the solution.

X. Interest

There is a natural fascination with developments of new technology. The integration of emerging technology in popular culture goes beyond its use in film and television, though. The evolution of artificial intelligence, biotechnology, and cybersecurity ripples through multiple industries which creates an increased interest in these technologies for the layperson. Artificial intelligence may seem like science fiction to a non-technical crowd, but it is finding greater relevance yearly. The ubiquity of Amazon Alexa and smart home devices prove the topical nature of artificial intelligence's role in most Americans' lives. Yet, not as many may be aware of the real threats posed by AI's use in military operations. Rural communities know well the

impact of biotechnology on the expansion of agricultural products to enhance yield. As technology progresses, there could be threats to crops from groups bent on disrupting the American system of agriculture using a synthesized biological weapon. Millions know the importance of cybersecurity as the transition to electronic information forces our sensitive personal information onto online databases. Will the next hack involve your bank information, your social security number, or perhaps your medical records? Of even greater concern to many Americans is the security of our critical infrastructure. If hackers are able to compromise the power grid, water treatment facilities, or satellite communications, our country could be brought to the brink of collapse. Emerging technologies and their dual-use require the delicate balance between policies which allow for innovation and those that regulate misuse. Students, judges, and community members will have much to learn during a round and possibly even more to discuss with one another after rounds have concluded.

XI. Possible Affirmative Cases and Negative Positions

Aff Cases

Regulate/Ban Autonomous Weapons
AI for International Supply Chains/Logistics
NATO Emerging Tech Investment Fund
AI Oversight Body
Regulate Facial Recognition
Vaccine Diplomacy
Agricultural Biotechnology Cooperation
Limit DNA Databases
Regulate CRISPR
Investment in Biofuels
Critical Cybersecurity Infrastructure
Layered Cyber Deterrence
Defend Forward Cyber Strategy
Strengthen norms and non-military cyber tools
Create a “Cyber State of Distress” and cyber response and recovery fund
Military Cyber Mission Force
Deterrence First Cyber Strategy
Name and Shame Cyber Deterrence

End Offensive Cyber Operations (OCO's)
International Legal Frameworks for Cyberspace - Military & Non- Military
NATO Cyberspace Operations Center Cooperation
NATO Industry Cyber Partnerships

Neg Positions

UN Counterplan
AI Partnership for Defense Counterplan
Bilateral Counterplans (i.e. Cooperate with China)
Unilateral Counterplan (i.e. USFG as sole agent of action)
Private Sector Counterplans
Public/Private Partnership Counterplan
Multipolarity Bad
NATO Bad
Innovation Turns
China Backlash
Technology Arms Race
Hegemony Bad
Offensive Cyber Operations Good
Cyber Deterrence Bad
Military PIC
Tech Industry Econ DA
Tech Innovation DA
Transnational Crime DA

XII. References

Allison, G. & Schmidt, E. (2020, August). Is China beating the U.S. to AI supremacy? Retrieved from https://www.belfercenter.org/publication/china-beating-us-ai-supremacy

American Society of Mechanical Engineers. (2020, October 19). National Security Commission on artificial intelligence (NSCAI) releases 2020 interim report and recommendations. Retrieved from https://www.asme.org/government-relations/capitol-update/national-security-commission-on-artificial-intelligence-releases-2020-interim-report-and-recommendations

Barnett, J. (2020, April 24). Why the Pentagon can't go it alone on AI. Retrieved from https://www.fedscoop.com/experts-urge-us-nato-not-to-go-it-alone-on-developing-artificial-intelligence/

Berlatsky, N. (2018, December 06). Is AI dangerous? Why our fears of killer computers or sentient 'Westworld' robots are overblown. Retrieved from https://www.nbcnews.com/think/opinion/ai-dangerous-why-our-fears-killer-computers-or-sentient-westworld-ncna943111

Borghard, E. D. (2020, December 09). Emerging technology and a reimagined U.S.-EU partnership. Retrieved from https://www.cfr.org/blog/emerging-technology-and-reimagined-us-eu-partnership

Castellanos, S. (2020, November 02). AI, quantum R&D funding to remain a priority under Biden. Retrieved from www.wsj.com/articles/ai-quantum-r-d-funding-to-remain-a-priority-under-biden-11604944800

Choi, E. C. (2019, December 17). Will algorithms make safe decisions in foreign affairs? Retrieved from https://www.diplomacy.edu/blog/will-algorithms-make-safe-decisions-foreign-affairs

Christie, E. H. (2020, November 24). Artificial Intelligence at NATO: dynamic adoption, responsible use. Retrieved from https://www.nato.int/docu/review/articles/2020/11/24/artificial-intelligence-at-nato-dynamic-adoption-responsible-use/index.html

Cicarelli, M. B. (2021, January 13). NATO's Financing Gap. Retrieved from https://www.americanprogress.org/issues/security/reports/2021/01/13/494605/natos-financing-gap/

Clinton, W. J. (2000, March 09). Full text of Clinton's speech on China trade bill. Retrieved from https://www.iatp.org/sites/default/files/Full_Text_of_Clintons_Speech_on_China_Trade_Bi.htm

The collection edge: Harnessing emerging technologies for intelligence collection. (2020, July 13). Retrieved from https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection?gclid=Cj0KCQiAvP6ABhCjARIsAH37rbTnOphDY0r6LlhaXyHYI9bbuQUF3vKVa-NRS_xQantBhjfPJiiDSNQaAuAlEALw_wcB

Congressional Research Service. (2020, November 10). Artificial intelligence and national security. Retrieved from https://fas.org/sgp/crs/natsec/R45178.pdf

Copeland, B. J. (n.d.). Artificial intelligence. Retrieved from https://www.britannica.com/technology/artificial-intelligence

Cyber defence: Reports. (n.d.). Retrieved from https://natolibguides.info/cybersecurity/reports

Department of Homeland Security. (n.d.). Science and technology: International partnerships Retrieved from https://www.dhs.gov/science-and-technology/st-icpo

DIGITALEUROPE Director General to advise NATO on emerging technologies. (2020, July 8). Retrieved from https://www.digitaleurope.org/news/digitaleurope-director-general-to-advise-nato-on-emerging-technologies/

Ellehuus, R. Morcos, P. "'Lifting Up Our Values at Home': How to Revitalize NATO's Political Cohesion," *Center for Strategic and International Studies*, **March 12, 2021,** accessed online June 18, 2021. https://www.csis.org/analysis/lifting-our-values-home-how-revitalize-natos-political-cohesion

Emerging technologies and national security. (2020, December 31). *American Foreign Policy Council.* Retrieved from https://www.afpc.org/publications/e-journals/emerging-technologies-and-national-security

Emerging technologies and national security: Russia, NATO, & the European theater. (2019, February 25). Retrieved from https://www.hoover.org/research/emerging-technologies-and-national-security-russia-nato-european-theater

Emerging technology definition must protect American innovation (n.d.) National Venture Capital Association. Retrieved from https://nvca.org/pressreleases/emerging-technology-definition-must-protect-american-innovation/

Engstrom, D. F. et al. (2020, February). Government by algorithm: Artificial intelligence in federal administrative agencies. Retrieved from https://www.ospi.es/export/sites/ospi/documents/documentos/Tecnologias-habilitantes/US_ACUS_Gov-by-Algorithm-report.pdf

Erlanger, S. (2020, November 30). NATO needs to adapt quickly to stay relevant for 2030, report urges. Retrieved from https://www.nytimes.com/2020/11/30/world/europe/nato-2030-russia-china.html

Erlanger, S., & Michael. (2021, June 14). Shifting Focus, NATO Views China as a Global Security Challenge. Retrieved from https://www.nytimes.com/2021/06/14/world/europe/biden-nato-china-russia.html

European defence & transatlantic security cooperation. (2019, June 12). Retrieved from https://www.gmfus.org/events/european-defence-transatlantic-security-cooperation

Fishman, E. & Simakovsky M. (2021, March 05). A three-step plan for reviving the transatlantic alliance. Retrieved from http://www.atlanticcouncil.org/blogs/new-atlanticist/a-three-step-plan-for-reviving-the-transatlantic-alliance/.

Ford, C. A. (2020, April 20). Al, human-machine interaction, and autonomous weapons: Thinking carefully about taking "killer robots" seriously. Retrieved from https://www.state.gov/wp-content/uploads/2020/06/T-Paper-Series-2-LAWS-FINAL-508.pdf

Ford, L. W., & Goldgeier, J. (2021, January 25). Retooling America's alliances to manage the China challenge. Retrieved from https://www.brookings.edu/research/retooling-americas-alliances-to-manage-the-china-challenge/

Fried, I. (2021, March 02). China will dominate AI unless U.S. invests more, commission warns. Retrieved from https://www.axios.com/china-will-dominate-ai-unless-us-invests-more-commission-warns-addaee06-cc72-4c46-98ad-2962c5f919e0.html

The future of NATO. (2020, August 10). Retrieved from https://www.iai.it/en/eventi/future-nato

The future of warfare and the role of new and emerging technologies: Recap. (2021, February 23). Retrieved from https://www.globsec.org/news/11341/

Galatas, I. (2017). The misuse and malicious uses of the new biotechnologies. *Annales des Mines - Réalités industrielles*, 1(1), 103-108. https://doi.org/10.3917/rindu1.171.0103

Gill, I. (2020, January 31). Whoever leads in artificial intelligence in 2030 will rule the world until 2100. Retrieved from https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/

Global Futures Intelligence System. (n.d.). Retrieved from http://www.millennium-project.org/projects/global-futures-intelligence-system/?gclid=Cj0KCQiAvP6ABhCjARIsAH37rbT9fdD3kOoY1jLgaQnJlsie8R3OwSpLdzg8Sf3IcSwJLvrnTOhsy6UaAty2EALw_wcB

Gordon, M. R., & Marson, J. (2020, December 01). NATO should expand its focus to include China, report says. Retrieved from https://www.wsj.com/articles/nato-should-expand-its-focus-to-include-china-report-says-11606820403

Gould, J. (2021, February 23). After SolarWinds, US needs to toughen cyber defenses, says Microsoft president. Retrieved from http://www.c4isrnet.com/2021/02/23/after-solarwinds-us-needs-to-toughen-cyber-defenses-says-microsoft-president/

Hanke Vela, J., Leali, G. & Moens, B. (2021, January 01). Germany's drive for EU-China deal draws criticism from other EU countries. *Politico.* Retrieved from https://www.politico.eu/article/germanys-drive-for-eu-china-deal-draws-criticism-from-other-eu-countries/

Hao, K. (2021, January 22). The Biden administration's AI plans: what we might expect. *Technology Review*, Retrieved from https://www.technologyreview.com/2021/01/22/1016652/biden-administration-ai-plans-what-to-expect/

Hass, R. & Balin, Z. (2019, January 10). US-China relations in the age of artificial intelligence. Retrieved from https://www.brookings.edu/research/us-china-relations-in-the-age-of-artificial-intelligence/

Heikkila, M. (2021, March 29). NATO wants to set AI standards. If only its members agreed on the basics. Retrieved from https://www.politico.eu/article/nato-ai-artificial-intelligence-standards-priorities/

Hill, S. (2020, April 27). AI's impact on multilateral military cooperation: Experience from NATO. Retrieved from https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ais-impact-on-multilateral-military-cooperation-experience-from-nato/3AEF22AA22550A10B75DD74A806D4D18

IBM. (n.d.) Artificial intelligence (AI). Retrieved from https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

Kamarck, E. (2018, November 29). Malevolent soft power, AI, and the threat to democracy. Retrieved from https://www.brookings.edu/research/malevolent-soft-power-ai-and-the-threat-to-democracy/

Kasapoglu, C. & Kirdemir, B. (2019, November 28). Artificial intelligence and the future of conflict. Retrieved from https://carnegieeurope.eu/2019/11/28/artificial-intelligence-and-future-of-conflict-pub-80421

Key takeaways from the launch of e-volume on cyber threats and NATO 2030. (n.d.). *The NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved from https://ccdcoe.org/news/2021/key-takeaways-from-the-launch-of-e-volume-on-cyber-threats-and-nato-2030/

Koblentz, G. D. (2020, June 16). Emerging technologies and the future of CBRN terrorism. *The Washington Quarterly*, *43*(2), 177-196, Retrieved from https://www.tandfonline.com/doi/abs/10.1080/0163660X.2020.1770969?journalCode=rwaq20

Kosal, M. E. (2020, January 13). NATO and emerging technologies. Retrieved from https://www.europeanleadershipnetwork.org/commentary/nato-and-emerging-technologies/

Kurup, V. M., & Thomas, J. (2020). Edible vaccines: Promises and challenges. *Molecular biotechnology*, 62(2), 79–90. https://doi.org/10.1007/s12033-019-00222-1

Lawrence, C. & Cordey, S. (2020, August). The case for increased transatlantic cooperation on artificial intelligence. Retrieved from https://www.belfercenter.org/publication/case-increased-transatlantic-cooperation-artificial-intelligence

Ledford, H. (2020, January 06). Quest to use CRISPR against disease gains ground. Retrieved from https://www.nature.com/articles/d41586-019-03919-0

Lee, M. (2021, March 03). Biden brings no relief to tensions between US and China. Retrieved from https://apnews.com/article/joe-biden-donald-trump-biden-cabinet-beijing-coronavirus-pandemic-060ee406fe2e488e524552c43083ddad

Leopold, G. (2020, November 02). NATO targets AI interoperability. Retrieved from https://www.enterpriseai.news/2020/11/02/nato-targets-ai-interoperability/

Lepido, D. (2021, March 23). Swiss Cyber Security Firm Says It Accessed Servers of a SolarWinds Hacking Group. *Insurance Journal*, Retrieved from https://www.insurancejournal.com/news/international/2021/03/23/606548.htm#:~:text=A%20Swiss%20cyber%2Dsecurity%20firm,their%20campaign%20through%20this%20month

LeVine, S. (2018, March 21). The stakes for who wins the AI race. Retrieved from https://www.axios.com/the-stakes-for-who-wins-the-ai-race-0363d9cd-0d97-4a5a-9ee6-36a7fb03ff44.html

Lin-Greenberg, E. (2020, March). Allies and artificial intelligence: Obstacles to operations and decision-making. Retrieved from https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/

Lomas, N. (2020, December 02). Europe will push to work with the US on tech governance, post-Trump. Retrieved from https://techcrunch.com/2020/12/02/europe-will-push-to-work-with-the-us-on-tech-governance-post-trump/

Mattox, G. (2020, February 27) The future of transatlantic security cooperation: Past successes and emerging threats. *American Institute for Contemporary German Studies*. Retrieved from https://www.aicgs.org/2020/02/the-future-of-transatlantic-security-cooperation-past-successes-and-emerging-threats/

Morcos, P. (2020, December 3). NATO in 2030: Charting a new path for the transatlantic alliance. *Center for Strategic & International Studies*. Retrieved from https://www.csis.org/analysis/nato-2030-charting-new-path-transatlantic-alliance

Markotkin, N. & Chernenko, E. (2020, August 05). Developing artificial intelligence in Russia: Objectives and reality. Retrieved from https://carnegie.ru/commentary/82422

Martinez, D. et al. (2019, January). Artificial intelligence: Short history, present developments, and future outlook. Retrieved from https://www.ll.mit.edu/sites/default/files/publication/doc/2019-09/Artificial%20Intelligence%20Short%20History%2C%20Present%20Developments%2C%20and%20Future%20Outlook%20-%20Final%20Report%20-%20Martinez.pdf

Metz, C. (2019, February 11). Trump signs executive order promoting artificial intelligence. Retrieved from https://www.nytimes.com/2019/02/11/business/ai-artificial-intelligence-trump.html

Moore, S. (2020, April). China's role in the global biotechnology sector and implications for US policy. *Brookings Institute*. Retrieved from https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_china_biotechnology_moore.pdf

Moore, S. (2021, February 17). In biotech, the industry of the future, the U.S. is way ahead of China." *Lawfare*, Retrieved from www.lawfareblog.com/biotech-industry-future-us-way-ahead-china.

Murphy, C., Stebbing, E. F., Pascal Kalume Kambale and Mvemba Phezo Dizolele, Takeyh, R., Segal, A., Wodu, N., . . . Editors, C. (2020, April 21). How to Understand Technology and Geopolitics. Retrieved from https://www.foreignaffairs.com/lists/2019-10-07/how-understand-technology-and-geopolitics

Murray, R. (2020, September 01). Building a resilient innovation pipeline for the alliance. Retrieved from https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/index.html

The National Intelligence Research and Development Strategic Plan: 2019 Update. (2019, June). Select Committee of Artificial Intelligence of the National Science & Technology Council, June 2019. https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf

NATO technology innovation conference is coming to Prague. (2020, February 11). Retrieved from https://spendmatters.com/uk/nato-innovation-conference-comes-to-prague/

NATO ACT. (n.d.). Retrieved from https://adlnet.gov/partnership-network/nato-allied-command-transformation-act-adl/

NATO. November 16, 2020. (n.d.), NATO readies for cyber threats. www.nato.int/cps/en/natohq/news_179481.htm?selectedLocale=en.

NATO and Europe in the 21st century: New roles for a changing partnership. (n.d.). Retrieved from https://www.wilsoncenter.org/publication/nato-and-europe-the-21st-century-new-roles-for-changing-partnership

North Atlantic Treaty Organization. (n.d.). Retrieved from https://www.rand.org/topics/north-atlantic-treaty-organization.html

Partnership for technology in peacekeeping (n.d.). *United Nations*. Retrieved from https://operationalsupport.un.org/en/partnership-technology-peacekeeping

Paun, C., & Heath, R. (2020, July 24). How the coronavirus can prepare us for bioterrorism. Retrieved from https://www.politico.com/news/2020/07/24/how-to-prepare-for-bioterrorism-courtesy-of-coronavirus-380689

Pepe, E. (2020, November 13). NATO and collective thinking on AI. Retrieved from https://www.iiss.org/blogs/military-balance/2020/11/nato-artificial-intelligence

Pomerleau, M., & Eversden, A. (2020, March 11). Congressional report outlines new American cyber strategy. Retrieved from

https://www.fifthdomain.com/congress/2020/03/11/congressional-report-outlines-new-american-cyber-strategy/

Prasad, K. (2021, April 05). Commentary: Unless the U.S. changes its vaccine policy, the world will look at us like hoarders. Retrieved from https://fortune.com/2021/04/04/us-vaccine-hoarding-nationalism-diplomacy-china-russia-india/

Remarks by President Biden at the 2021 Virtual Munich Security Conference. (2021, February 19). Retrieved from http://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/19/remarks-by-president-biden-at-the-2021-virtual-munich-security-conference/

Report. (n.d.). Retrieved from https://www.solarium.gov/report

Reynolds, J. & Lightfoot, J.. (2020, October 14). Digitalize the enterprise. Retrieved from https://www.atlanticcouncil.org/content-series/nato20-2020/digitalize-the-enterprise/

Richardson, L. C. et al. (2019, Jun 6). Cyberbiosecurity: A call for cooperation in a new threat landscape. *Frontiers in Bioengineering and Biotechnology 7*(99), doi:10.3389/fbioe.2019.00099

Riley, T. (2021, Match 26). Analysis | The Cybersecurity 202: NSA Director Says Intelligence Has a Big Blind Spot: Domestic Internet Activity. *The Washington Post*, Retrieved from www.washingtonpost.com/politics/2021/03/26/cybersecurity-202-nsa-director-says-intelligence-has-big-blind-spot-domestic-internet-activity/#click=t.co/kg8XkfRoXH.

Sanger, D. E., Erlanger, S., & Cohen, R. (2021, February 20). Biden Tells Allies 'America Is Back,' but Macron and Merkel Push Back. Retrieved from https://www.nytimes.com/2021/02/19/us/politics/biden-munich-conference.html

Sanger, D. E. & Kramer, A. E. (2021, April 16). U.S. imposes stiff sanctions on Russia, blaming it for major hacking operation. *New York Times*. Retrieved from http://www.nytimes.com/2021/04/15/world/europe/us-russia-sanctions.html

Schwartz, O. (2018, July 25). 'The discourse is unhinged': how the media gets AI alarmingly wrong. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/jul/25/ai-artificial-intelligence-social-media-bots-wrong

Select committee on artificial intelligence of the National Science & Technology Council. (2019, June). Retrieved from https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.p

Shalal, A. (2018, November 13). NATO looks to startups, disruptive tech to conquer emerging threats. Retrieved from https://www.reuters.com/article/us-nato-innovation/nato-looks-to-startups-disruptive-tech-to-conquer-emerging-threats-idUSKCN1NI2NW

Sharper: America's alliances and partnerships. (n.d.). Retrieved from https://www.cnas.org/publications/commentary/sharper-americas-alliances-and-partnerships

Shea, J. and Williams, M. The secret to NATO's survival: Get political. (2021, June 17). Retrieved from https://www.atlanticcouncil.org/blogs/new-atlanticist/the-secret-to-natos-survival-get-political/

Shead, S. (2021, March 02). U.S. is ‘not prepared to defend or compete in the A.I. era,’ says expert group chaired by Eric Schmidt. *CNBC*. Retrieved from https://www.cnbc.com/2021/03/02/us-not-prepared-to-defend-or-compete-in-ai-era-says-eric-schmidt-group.html

Sherman, J. & Hu, E. (2021, February 19). How the next National Defense Strategy can get serious about emerging technologies. *Atlantic Council*, Retrieved from www.atlanticcouncil.org/blogs/new-atlanticist/how-the-next-national-defense-strategy-can-get-serious-about-emerging-technologies/.

Should we fear artificial intelligence? (2018, March). Retrieved from https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614547/EPRS_IDA(2018)614547_EN.pdf

Soare, S. R. (2020, March). Digital divide? Transatlantic defence cooperation on Artificial Intelligence. Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%203%20AI_0.pdf

Speranza, L. (2020, November 9). An agenda for NATO's next generation. Retrieved from https://cepa.org/an-agenda-for-natos-next-generation/

Speranza, L., & Nelson, N. (2020, December 08). NATO needs a strategy for emerging and disruptive technologies. Retrieved from https://www.defensenews.com/opinion/2020/12/08/nato-needs-a-strategy-for-emerging-and-disruptive-technologies/

Stavridis, J. (2019, April 04). Why NATO is essential for world peace, according to its former commander. Retrieved from https://time.com/5564171/why-nato-is-essential-world-peace/

Straub, J. (2018, January 29). Artificial intelligence is the weapon of the next Cold War. Retrieved from https://theconversation.com/artificial-intelligence-is-the-weapon-of-the-next-cold-war-86086

Swejis, T. & Osinga, F. (2020, April 04). Maintaining NATO's technological edge. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/02681307.2019.1731216?scroll=top&needAccess=true&journalCode=rwhi20

Tadjdeh, Y. (2020, March 03). DoD seeks AI alliance to counter China, Russia. Retrieved from https://www.nationaldefensemagazine.org/articles/2020/3/3/algorithmic-warfare-dod-seeks-ai-alliance-to-counter-china-russia

Tellier, K. (2021, March 29). March 29, 2021: Reading notes: Ryan Hass's 'competitive interdependence'. Retrieved from https://kevtellier.substack.com/p/march-29-2021-reading-notes-ryan

Tucker, P. (2021, June 22). NATO Members Agree to Broad Tech, Environmental Agenda. Retrieved from https://www.defenseone.com/threats/2021/06/nato-members-agree-broad-tech-agenda-environmental-agenda/174767/

U.S. body on artificial intelligence calls for creating India-US strategic tech alliance. (2020, October 14). Retrieved from https://economictimes.indiatimes.com/news/defence/us-body-on-artificial-intelligence-calls-for-creating-india-us-strategic-tech-alliance/articleshow/78659333.cms?from=mdr

U.S. security cooperation with Finland. (2021, January 20). *United States Department of State* Retrieved from https://www.state.gov/u-s-security-cooperation-with-finland/

Ventura, T. (2021, January 10). How NATO's emerging culture of innovation is reshaping the alliance. Retrieved from https://medium.com/predict/how-natos-emerging-culture-of-innovation-is-reshaping-the-alliance-1b7f8023f393

Verma, A. S., Agrahari, S., Rastogi, S., & Singh, A. (2011). Biotechnology in the realm of history. Journal of pharmacy & bioallied sciences, 3(3), 321–323. https://doi.org/10.4103/0975-7406.84430

Vogel, K. M., & Ouagrham-Gormley, S. B. (2018). Anticipating emerging biotechnology threats: A case study of CRISPR. *Politics and the Life Sciences*, *37*(2), 203-219. https://doi.org/10.1017/pls.2018.21

Walla, K. et al. (2020, October 29). The transatlantic alliance needs to work together to gain technological edge. *Atlantic Council*. Retrieved from https://www.atlanticcouncil.org/blogs/new-atlanticist/the-transatlantic-alliance-needs-to-work-together-to-gain-technological-edge/

Webinar: How do emergent and disruptive technologies shape the security agenda in the South? (n.d.). Retrieved from https://thesouthernhub.org/activities/webinar-how-do-emergent-and-disruptive-technologies-shape-the-security-agenda-in-the-south

Weiss, S. (April 2016) "Harnessing biotechnology: A practical guide." Chemical Engineering. Retrieved from https://www.genomatica.com/wp-content/uploads/2017/01/Harnessing-Biotechnology-A-Practical-Guide.pdf

West, R. M., & Gronvall, G. K. (2020). CRISPR cautions: Biosecurity implications of gene editing. *Perspectives in Biology and Medicine*, 63(1), 73-92. doi:10.1353/pbm.2020.0006

Wiggers, K. (2020, November 06). How AI predictions fared against pollsters in the 2020 U.S. election. Retrieved from https://venturebeat.com/2020/11/06/how-ai-predictions-fared-against-pollsters-in-the-2020-u-s-election/

Wright, N. (2018, July 10). How artificial intelligence will reshape the global order.

Retrieved from https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order?utm_medium=email_notifications&utm_source=reg_confirmation&utm_campaign=reg_guestpass

Zandee, D. (n.d.) The future of NATO: Strategic monitor 2018-2019. *Clingendael.* Retrieved from https://www.clingendael.org/pub/2018/strategic-monitor-2018-2019/the-future-of-nato/