# Unilat CP

## 1NC

### 1NC Counterplan Text - Public-Private

#### Counterplan: The United States Federal Government should not substantially increase its security cooperation with the North Atlantic Treaty Organization in [AFF areas] and should substantially increase its support for security capability development in [aff areas] by increasing research and development funding and encourage public-private partnership development through the Department of Defense.

## Solvency

### S – Generic

#### Private-public collaboration is key to developments in AI, biotech, and cyber

Heckman 22 (Jory Heckman - Jory Heckman is a reporter at Federal News Network covering U.S. Postal Service, IRS, big data and technology issues. “Federal R&D investments serve as foundation for US becoming AI-ready," Federal News Network, 4-12-2022 https://federalnewsnetwork.com/artificial-intelligence/2022/04/federal-rd-investments-serve-as-foundation-for-us-becoming-ai-ready/?readmore=1) CL

The National Security Commission on Artificial Intelligence, in its [final report to Congress and the Biden administration](https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf) last year, warned artificial intelligence will soon become “weapons of first resort in future conflicts.”) CL

That warning, as well as the commission’s recommendation for the federal government to increase spending on basic research and development, remains urgent for the U.S. to remain AI-ready in the coming years, even though the commission no longer remains. The commission disbanded in October 2021, but many of its leading experts have shifted to a private-sector entity, the [Special Competitive Studies Project](https://www.scsp.ai/) (SCSP). The name stems from the Rockefeller Special Studies Project, launched in 1956 by Nelson Rockefeller and Henry Kissinger following the Soviet Union’s launch of the satellite Sputnik. SCSP chief executive officer Ylli Bajraktari, NSCAI’s former executive director, said Rockefeller and Kissinger saw their project as a way for the U.S. to further define its national objectives when it came to defense, security and foreign policy. “This is not the first time that we’re seeing technology playing a critical role in great power competition,” Bajraktari said. That mission, he added, remains urgent in the present day. Unlike the Cold War era, however, when the federal government played a leading role in research and development**, the private sector is now the driving force in R&D spending.** Bajraktari said **the private sector’s R&D spending has obvious impacts on society and the public**, but also holds major implications for national security. “That’s why this is such a critical time, because of the diffusion of power, the diffusion of technologies and accessibility. Not just the United States government has access to these technologies. Anybody can purchase these kinds of capabilities off the shelf or online. This is a new momentum in how conflicts are waged, how geopolitics will be formed,” Bajraktari said. To prepare for the next era of great power competition, Bajraktari said the federal government will need to increase its level of spending on basic R&D. NSCAI in its final report urged Congress to double federal R&D spending for AI each year, until it reached $32 billion in fiscal 2026. The Biden administration**,** [**in its fiscal 2023 budget request**](https://www.whitehouse.gov/wp-content/uploads/2022/04/ap_18_research_fy2023.pdf)**, proposes increasing the federal R&D budget to more than $204 billion, a 28% increase from FY 2021 enacted levels**. Part of that funding would support new and existing National AI Research Institutes. These institutes bring federal, state and local agencies together with the private sector, nonprofits and academia to tackle AI research and workforce development challenges. “If we don’t outmaneuver and not out-innovate China, we will not be in the lead position when it comes to these emerging technologies. The lead position in emerging technologies ensures that our economy keeps progressing, that our society is using all the benefits from these technologies, and ultimately, our military has the latest and greatest capabilities, if they need to utilize it for warfighting purposes,” Bajraktari said. Meanwhile, the National Science Foundation’s National Science Board finds the U.S. remains strong in terms of global R&D competition, but global competitors are catching up. Victor McCrary, NSB’s vice chairman and the vice president for research and graduate programs at the University of the District of Columbia, said the U.S. “still outpaces everybody in terms of overall global R&D.” However, McCrary said South Asian and Southeast Asian countries, particularly China, have been increasing R&D spending in recent years. “While the U.S. leads, that margin between us and our nearest competitors is starting to close, and I think that’s a concern from the White House to the Congress, to many of our business, universities, as well as the military,” McCrary said. McCrary said **basic R&D serves as the foundation for breakthroughs in artificial intelligence, quantum information systems, 5G, biotechnology and advanced manufacturing**. The National Science Board, under the National Science Foundation Act, is required to send Congress and the president a report on the state of science and engineering every even-numbered year. This [year’s report shows](https://ncses.nsf.gov/pubs/nsb20221) that in addition to being a top global spender on R&D, the U.S. maintains a competitive advantage by still drawing the best talent to its universities and companies. McCrary said this talent pool gives the U.S. an international advantage. “We still have the best companies in the world when it comes to AI applications and integration of these things,” he said. Bajraktari said maintaining a high level of R&D spending is also a vital part of developing the STEM workforce necessary to remain competitive. “If these are our comparative advantages, then I think basic R&D can help towards incentivizing students and Ph.D. candidates at universities to come up with next-generation AI capabilities,” Bajraktari said. However, Bajraktari said federal agencies need to do a better job of ensuring private-sector tech experts have opportunities to lend their expertise to the government through short-term tours of duty. Meanwhile, he said the Defense Department and the intelligence community need to develop clearer career pathways for AI and emerging tech experts to stay in federal service. “The career path inside a federal agency is not clear-cut if you have a technology background. Until yesterday, this was considered an IT issue, but this is no longer an IT issue. **We need the military to understand** that if somebody comes with a coding background, **you have to incentivize** them and create a career pathway **for them to stay there and get promoted and get incentivized** — not move them around every two-to-three years, like we do right now. Because otherwise, you will lose the benefit of these individuals coming with these skills,” Bajraktari said.

### S – AI

#### Public-private partnership is key to AI

Sayler 20, (Kelley M. Sayler, Analyst in Advanced Technology and Global Security, November 10 2020, Congressional Research Service, “Artificial Intelligence and National Security”, https://sgp.fas.org/crs/natsec/R45178.pdf)

Some reports indicate that DOD and the defense industry also face challenges when it comes to recruiting and retaining personnel with expertise in AI due to research funding and salaries that significantly lag behind those of commercial companies.121 Other reports suggest that such challenges stem from quality-of-life factors, as well as from a belief among many technology workers that “they can achieve large-scale change faster and better outside the government than within it.” 122 This sentiment echoes the findings of the National Security Commission on Artificial Intelligence, which notes that “AI experts would be willing to serve in government if officials could create a more compelling sense of purpose and a technical environment within government that would maximize their talents.” 123 Regardless, observers note that if DOD and defense industry are unable to recruit and retain the appropriate experts, military AI applications could be delayed, “deficient, or lacking in appropriate safeguards and testing.” 124 To address these challenges, the Obama Administration launched the Defense Digital Service in 2015 as a means of recruiting private sector technology workers to serve in DOD for one to two year assignments—a “tour of duty for nerds,” according to former director Chris Lynch. 125 Similarly, former Deputy Secretary of Defense Bob Work has proposed an “AI Training Corps,” in which DOD “would pay for advanced technical education in exchange for two days a month of training with government systems and two weeks a year for major exercises.” Participants in the program could additionally be called to government service in the event of a national emergency.126 Other analysts have recommended the establishment of new military training and occupational specialties to cultivate AI talent, as well as the creation of government fellowships and accelerated promotion tracks to reward the most talented technology workers.

#### The Department of Defense needs to develop AI technology

Gao 22, (GAO-22-105834, Mar 30, 2022, “Artificial Intelligence: DOD Should Improve Strategies, Inventory Process, and Collaboration Guidance”, https://www.gao.gov/products/gao-22-105834)

The Defense Department believes that artificial intelligence will transform warfare, and failure to adopt AI technology could hinder national security. DOD is making organizational changes and investing billions of dollars to incorporate AI technology. We found that DOD's AI-related strategies could be more comprehensive, such as by including full descriptions of the resources needed for developing AI-enabled technologies. In addition, DOD has not yet issued guidance that clearly defines the roles and responsibilities of components that participate in AI activities. Our 7 recommendations address these and other issues. The 2018 Department of Defense (DOD) Artificial Intelligence (AI) Strategy defines AI as the ability of machines to perform tasks that normally require human intelligence. The strategy and associated plans include some, but not all, characteristics of a comprehensive strategy. For example, DOD's nine AI-related strategies and plans do not include full descriptions of resources and investments and risk associated with adoption of AI-enabled technologies. Issuing guidance to include all characteristics of a comprehensive strategy in future AI-related strategies could help DOD be better positioned to help managers ensure accountability and responsible use of AI. Assessment of DOD Artificial Intelligence-Related Strategies and Plans Assessment of DOD Artificial Intelligence-Related Strategies and Plans DOD has begun to identify and report on its AI activities, but limitations exist in its AI baseline inventory, such as the exclusion of classified activities. DOD officials said these limitations will be addressed in subsequent phases of the AI inventory identification process. However, DOD has not yet developed a high-level plan or roadmap that captures all requirements and milestones. Such a plan would provide DOD with a high-level, end-to-end view of all the features necessary to accomplish the program's goal to provide a complete and accurate inventory of AI activities to Congress and to DOD decision makers. DOD organizations collaborate on AI activities, but can more fully incorporate leading collaboration practices. DOD uses a variety of formal and informal collaborative mechanisms that GAO's prior work has identified, such as interagency groups. DOD has partially incorporated leading collaboration practices, such as identifying leadership. However, DOD officials told us they are in the process of developing guidance and agreements that clearly define the roles and responsibilities of DOD components that participate in AI activities. By finalizing and issuing such guidance, DOD could help ensure all participants agree upon responsibilities and decision making on AI efforts across the department. Why GAO Did This Study DOD strategies state that AI will transform the character of warfare, and failure to adopt AI technology could hinder the capability of warfighters to defend our nation. DOD is making organizational changes and investing billions of dollars to incorporate AI technology, such as establishing the Joint AI Center to accelerate the delivery of AI-enabled capabilities across DOD. House Report 116-442 accompanying the National Defense Authorization Act for Fiscal Year 2021, includes a provision for GAO to assess DOD's resources, capabilities, and plans for AI technology. This report evaluates the extent to which (1) DOD's AI Strategy and associated plans include characteristics of a comprehensive strategy; (2) DOD has identified and reported AI activities across the department; and (3) DOD collaborates on its AI activities. GAO reviewed relevant laws and DOD strategies that outline plans and processes to manage AI across the department, interviewed officials, and conducted a department-wide survey. This is a public version of a sensitive report that GAO issued in February 2022. Information that DOD deemed sensitive has been omitted.

#### US AI development fulfills US defense goals

Gill 22 [Jaspreet Gill. "A new $200M fund could help COCOMs with AI adoption". 3-17-2022. Breaking Defense. https://breakingdefense.com/2022/03/a-new-200m-fund-could-help-cocoms-with-ai-adoption/. 7-3-2022.] -AL

WASHINGTON: A new artificial intelligence fund tucked away in the $1.5 trillion fiscal 2022 spending package signed by President Joe Biden this week could aid the Pentagon in its efforts to increase adoption of AI at the combatant command level. The $200 million Artificial Intelligence and Development Fund is meant to improve tactical AI at combatant commands. However, according to budget documents, congressional defense committees want a briefing by Defense Secretary Lloyd Austin on an “execution plan” before the Pentagon can lay hands on any of the funding. The new fund aligns with the Defense Department’s AI efforts, notably the AI and Data Acceleration initiative announced last year by Deputy Defense Secretary Kathleen Hicks. Under the effort, operational data and AI flyaway teams of technical experts are being sent to the military’s 11 COCOMs to help them better understand their data and create AI tools to streamline decision-making. DoD wants to use the information gathered from the teams and COCOMs to “update its network infrastructure, remove policy barriers and ensure the reliability and effectiveness of its global warfighting capabilities,” according to a June 2021DoD memo announcing the initiative. The effort involves the services as well as key Pentagon agencies like the Joint Artificial Intelligence Center, which is developing a joint operating system for COCOMs build and field AI algorithms rapidly. This “integration layer” will be the first of its kind for DoD, JAIC Director Lt. Gen. Michael Groen told Breaking Defense in February. The Navy also revealed its own involvement in the effort at the WEST 2022 conference in San Diego in February. Duncan McCaskill, the Navy’s chief analytics officer, told the audience the service had sent one of its data engineers out to a shipyard to help personnel at EUCOM work through a use case for three months. As of February, DoD had completed its first round of assessments at the COCOMs. The $1.5 trillion funding package also contains $50 million to improve recruitment and development of AI talent, $70 million to increase DARPA’s AI, cyber and data analytics efforts, $23 million to improving training at US Cyber Command and $62 million to strengthen DoD networks from cyber threats.

### S – Cyber

#### Public-private relationship is critical for protecting critical infrastructures against cyber attacks

Brooks 19 (Chuck Brooks - President of Brooks Consulting International. “Public Private Partnerships And The Cybersecurity Challenge Of Protecting Critical Infrastructure.” Forbes. May 6, 2019. https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/?sh=134a6ca25a57.)

In the U.S., most of the critical infrastructure, including defense, oil and gas, electric power grids, health care, utilities, communications, transportation, education, banking and finance, is owned by the private sector (about 85 percent according to DHS) and regulated by the public sector. The public and private relationship in operating and protecting critical infrastructure requires a strong working partnership. Protecting the critical infrastructure poses a difficult challenge because democratic societies by their nature are interactive, open and accessible. Because of the growing digital connectivity (and interdependence) of both IT and industrial control systems, critical infrastructure is facing an evolving and sophisticated array of cybersecurity challenges. A recent survey of professionals in industries using industrial control systems (ICS) and operational technology (OT) commissioned by Tenable from the Ponemon Institute found that 90 percent of respondents say their environment has been damaged by at least one cyberattack over the past two years, with 62 percent experiencing two or more attacks. The survey of security professionals also revealed that nine in 10 critical infrastructure providers have experienced cyberattacks that rendered their systems out of action in the last two years. Director of National Intelligence Dan Coats recently stated that “the threat was growing for a devastating cyber assault on critical U.S. infrastructure, saying the ’warning lights are blinking red again‘ nearly two decades after the Sept. 11, 2001, attacks”. Critical infrastructure is the core of our nations’ prosperity and well-being and addressing the threats to it requires incorporating a robust calculated security strategy of public and private sector partnering. Cybersecurity relies on the same security elements for protection as physical security: layered vigilance, readiness and resilience. For example, energy security and the power grid requires private public cooperation and regulatory coordination among industry and Department of Homeland Security (DHS), Department of Energy (DOE), and the Department of Defense (DOD). The power grid and other industrial infrastructure have been increasingly subjected to both physical and cybersecurity attacks in recent years. According to Israel Barak, CISO at Cybereason, "most countries are still vulnerable to cyber-attacks on critical infrastructure because the systems are generally old and poorly patched. Power grids are interconnected and thus vulnerable to cascading failures.” Protecting critical ICS, OT, and IT systems from cybersecurity threats is a difficult endeavor. They all have unique operational frameworks, access points, and a variety of legacy systems and emerging technologies. The explosion of connected devices comprising the Internet of Things and the Industrial Internet of Things is daunting. The trends of integration of hardware and software combined with growing networked sensors are redefining the surface attack opportunities for hackers across all digital infrastructures. According to the DHS Alert (TA17-293A) threat actors have targeted government entities and the energy, water, aviation, nuclear, and critical manufacturing sectors since at least 2017 and, in some cases, have leveraged their capabilities to compromise victims’ networks. Historically, cyber threat actors have targeted the energy sector with various results, ranging from cyber espionage to the ability to disrupt energy systems in the event of a hostile conflict. Analysis by DHS, FBI, and trusted partners has identified distinct indicators and behaviors related to this activity. It's a global threat not just against the United States. In 2017, Hackers use Triton, a specialized malware to compromise critical safety systems at Schneider Electric. The malware is still being used to target industrial systems. Because of the sensitivity to the threats to national security and changing threat matrix of hackers augmented by newer technologies such as machine learning and artificial intelligence, the government is prioritizing the importance of the risk management approach to defend against more sophisticated malware and automated attacks targeting critical infrastructure. An effective risk management approach necessitates information sharing that helps allow government and industry to keep abreast of the latest viruses, malware, phishing threats, ransomware, insider threats, and denial of service attacks. Information sharing also establishes working protocols for lessons-learned and resilience that is critical for the success of mitigating incidents. A cornerstone of that approach is creating Public Private Partnerships (PPP) based upon risk management frameworks. A high level of public-private collaboration is needed to address growing cyber-threats. Preparation and commitment from both government and industry leadership is critical. Industry should collaborate with government to best utilize risk management models and prepare resiliency plans. The specifics of an industry security approach may vary according to circumstances, but the mesh that connects the elements is situational awareness combined with systematic abilities for operational management and critical communications in cases of emergency. In the federal civilian sector DHS’s new agency, Critical Infrastructure Security Agency (CISA) puts a keen focus on DHS’s integral role in cyber preparedness, response and resilience for critical infrastructure. DHS has identified 16 infrastructures deemed critical because their physical and digital assets, systems, and networks are considered vital to national economic security, safety and national public health. CISA’s stated role is to coordinate “security and resilience efforts using trusted partnerships across the private and public sectors, and deliver training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.” At DOD, Former Commander of the U.S. Cyber Command and former Director of the National Security Agency hailed the importance of the public-private cybersecurity partnership stating that “collaboration is critical given growing threats to everyone from cyberspace.” DOD and the National Security Agency (NSA) are working closely with the private sector in information sharing and in developing solutions to evolving threats. Whether the U.S. critical infrastructure protection security mission includes DHS, DOD, DOE, the intelligence community, or other government agencies, a public/private security strategy to meet growing challenges needs to be both comprehensive and adaptive. The same formula applies to other democratic nations sharing operations across industries and infrastructure.

#### **Public-private partnership is the key to preventing future cyber attacks**

Reilly 21 (Dan Reilly – journalist and editor. “Cybersecurity experts say public-private partnership is the key to preventing future attacks.” Fortune. November 16, 2021. https://fortune.com/2021/11/16/cybersecurity-future-government-corporation-partnership-data-breach/)

The number of data breaches through the third quarter of 2021 is up 17% over the previous year combined, according to the Identity Theft Resource Center. A study by IBM and the Ponemon Institute says the cost of the average data breach is up to $4.24 million, up from $3.86 million in 2020. Some estimates say cyberattacks could cost businesses and government agencies $6 trillion in 2021 alone, with that number rising dramatically in the years to come. With hacks coming from foreign governments and small groups of cybercriminals alike, a question remains—who’s responsible for preventing these attacks, the government or the corporations? According to Kiersten Todt, the Chief of Staff of the Cybersecurity and Infrastructure Security Agency, a federal agency operating under the Department of Homeland Security, the only way forward is to have businesses and the government fighting this digital war together. That’s why CISA launched the Joint Cyber Defense Collaborative initiative in August, a public-private partnership to help boost cybersecurity with Amazon, Google, and Microsoft all taking part. “What this is doing is sort of taking that approach and turning it on its side because it's really about operational collaboration,” Todt said at the Fortune CEO Initiative conference in Washington, D.C. on Tuesday. “I've had a lot of thinking around, 'Is this a concept that could have succeeded a few years ago?' and I'm not actually sure that it could have because one of the things that SolarWinds demonstrated was that the private sector has enormous intelligence capability on each of its own companies. Government has capabilities in understanding nation-state activity.” Todt noted the marriage of government and corporate capabilities to detect, prevent, and share information about an attack before it happens is at the heart of operational collaboration. ”This operational collaboration has already been put into effect and has had some successes, and it is going to expand out to different companies,” said Todt. This **public-private partnership is crucial**, according to Christian Brose, the Chief Strategy Officer of the defense tech company Anduril Industries. “When I was in government three years ago, the thing that we were all struggling with was, 'Who is responsible for what?’” he said. “‘When is a private company responsible for defending itself in this kind of gray zone? Is it really responsible for defending itself when it's being attacked by a pure adversary with nation-level capability?' At what point does the government really have to take responsibility for that? So the ability to actually begin marrying [these efforts], in an operational sense, is super important.” “That's so important, because when we were just talking about this before, a few years ago,we recognized that cyber is the only domain where we ask industry to defend itself,” Todt added. “Having that type of pre-event work so that you're not, in a time of crisis, trying to figure out where the marks are for who does what but there's actually a benefit to working together and it's not seen as a penalty is an important step in progress.” It’s an urgent development, Brose said, because we’re past the time to be worrying about eventualities in cybersecurity. “The thing that I would sort of underscore here is the future is now, the future is not coming,” he said, noting that there are cheap drones and A.I.-enabled weapons being used in conflicts around the world. “We oftentimes talk about getting ready for the future, and I would argue we've actually already been ambushed by it.”

#### New cyber framework must have public-private partnership, info sharing, shared action, and regulations

Jason Smith, 2-22-2022, Jason Smith currently serves as service chair and as assistant professor for security studies at the National War College. He has served as a leader and aviator in the US Coast Guard and the US Army, as advisor to the commandant of the Coast Guard, as senior policy advisor in the US Senate, and on the staff of the National Security Council. "Forget a Whole-of-Government Cybersecurity Strategy—It’s Time for a Whole-of-Nation Approach," Modern War Institute, <https://mwi.usma.edu/forget-a-whole-of-government-cybersecurity-strategy-its-time-for-a-whole-of-nation-approach/> //jsam

A whole-of-nation **strategy needs to have clear objectives** that are easily understood and actionable by the public and private sectors for the good of the American people. These objectives should include resiliency, redundancy, hardening, investigation, and sharing of information as a minimum. To meet those objectives a **whole-of-nation strategic framework requires: True public-private partnership.** This requires not only the **private sector to trust the government** with information that they consider vital, but also that the **government must trusts the private sector with the information it needs**. **This means an equal exchange of information**. **Sharing ideas, techniques, and technology.** Shared information about attacks themselves is only part of it. Allowing for a sharing of ideas, techniques, and technology is just as important. The government cannot afford to attract all the cyber experts into government jobs, nor should it want to; it needs the innovation and energy of the private sector. Bringing that innovation into the fold creates resources to counter our adversaries. Many in the private sector see the government as the enemy and their employees, shareholders, and customers protest when they partner with the government. This must be overcome by establishing a trusting environment. **Shared action. The strategy may limit offensive cyber activities to government agencies, or it may include a limited licensing to a few trusted companies.** This would not be as much a letter of marque as an avenue to seek permission to take one-time action on a target. Either way, all involved need to have visibility on actions taken and a voice—especially when it is the private sector that might take the brunt of any retaliation. **Regulations.** Although it is not popular with the private sector**, government regulation will be required**. Without it, incentives will not change and information sharing and investment in sound defenses will be hampered. **Other nations will continue to see cyberattacks on both government and private sector targets as a cheap and effective way to counter the United States.** The current whole-of-government response is full of noble intent, but it is not a winning strategy. It fails to take advantage of the resources and expertise in the private sector that a whole-of-nation response can. The United States’ free economy, and the incentives it brings, gives it a **competitive advantage over its adversaries, but only if it actively engages with private sector actors** and convinces them that a whole-of-nation response is in their best interest.

#### Only working with both public and private sectors solves

Jason Smith, 2-22-2022, Jason Smith currently serves as service chair and as assistant professor for security studies at the National War College. He has served as a leader and aviator in the US Coast Guard and the US Army, as advisor to the commandant of the Coast Guard, as senior policy advisor in the US Senate, and on the staff of the National Security Council. "Forget a Whole-of-Government Cybersecurity Strategy—It’s Time for a Whole-of-Nation Approach," Modern War Institute, <https://mwi.usma.edu/forget-a-whole-of-government-cybersecurity-strategy-its-time-for-a-whole-of-nation-approach/> //jsam

Response Companies are pressuring government officials for a solution, or at least more freedom to act themselves. The government is not ignoring the problem, but countering cyberattacks requires not only the technical capability to hack back; it also involves understanding a complex web of attribution and considerations governing the use of force, law enforcement, policy, and obligations to protect the innocent. While many companies would like to take a more active role in punishing those caught hacking their systems, this might cause more harm than good. However, discounting private companies is also a mistake. Subscribing to social contract theory does not mean that private citizens do not have a role to play in ensuring societal well-being. Juries are made up of everyday citizens and private think tanks routinely advise the government on security issues. The social contract in a democracy must be participatory. In fact, it is this participation in the government that gives democracies their strength. Participation brings new ideas, energy, and accountability. **A successful cyber posture that both defends against attacks and punishes those that are successful will take a concerted effort by government and the private sector. The government needs to take a lead in developing and executing a competitive strategy that bridges the public-private divide and increases the United States’ advantage**. But what form should that partnership take? Ought offensive or defensive approaches be prioritized?

#### Private sector can tackle cyber threats if US increases data sharing.

Shah and Sridhar 22 (Raj M. Shah and Kiran Sridhar. Shah is Chairman of Resilience Insurance and Managing Partner at Shield Capital. Sridhar is a risk researcher at the University of Cambridge. “How to Cyberproof the Private Sector.” Foreign Affairs. January 13, 2022. <https://www.foreignaffairs.com/articles/north-america/2022-01-13/how-cyberproof-private-sector>)

To address the current cybersecurity deficit, the U.S. government will need to facilitate far **greater sharing of** intelligence **data** **about** **cyberthreats** **throughout the economy**. Congress can do this by passing legislation to overhaul the Cybersecurity and Infrastructure Security Agency’s (CISA) information-sharing program, the Automated Indicator Sharing (AIS) initiative, and by establishing the Bureau of Cyber Statistics to regularly publish security data. But information alone will not solve the current cybersecurity crisis. A comprehensive cyberdefense strategy will also require new ways of getting companies themselves to act quickly on the most important threats and to put in place the best defenses. Under prevailing market forces, there is a strong **disincentive for cybersecurity firms to share information about threats**. Although many of these firms have gathered rich data about the vulnerabilities and relative security of common software products, they do not share this intelligence with the end users of these products for fear it would erode their competitive advantage. As a result, most companies are ill-equipped to evaluate the security risks of the software they depend on. The Israeli firm Cybersixgill has estimated that 90 percent of company chief information security officers make cybersecurity decisions based on outdated intelligence data. And **since there is very little information sharing, cyberattackers are often able to exploit the same vulnerability over and over** again to inflict damage on thousands of enterprises around the world. Since companies are not basing their purchase decisions on an accurate assessment of risks, there is little incentive for software providers to emphasize cybersecurity. Software products that are designed with enhanced security features are rarely able to command a premium, and many software companies have made the rational calculation that putting expensive resources into cybersecurity will not be rewarded by the market. Nor do they tend to suffer when their products are attacked. After all, as computer scientists Ross Anderson and Tyler Moore have pointed out, the clients of software companies—not the software companies themselves—are the ones that bear most of the costs of a cybersecurity failure. Meanwhile, companies are often reluctant to disclose cyberattacks when they occur, for fear of damaging their reputations––or worse, subjecting themselves to litigation. That reticence allows malicious hackers to reuse the same methods elsewhere. And cyber insurers, firms who write insurance policies to cover financial losses sustained by data breaches and digital disruptions, are similarly unwilling to share information about the efficacy of particular security defenses, which they view as proprietary. As a result, many **companies make critical cybersecurity investment decisions based on marketing or word of mouth rather than hard data**. **If information about threats were quickly shared around the world, cyberattacks would immediately lose much of their potency**. Companies would be able to quickly prioritize and address urgent security flaws within their digital networks or operating systems and malign actors would no longer be able to exploit a single vulnerability to attack a large number of targets. But to date, the government has struggled to overcome built-in resistance in the private sector to information-sharing about cyberthreats.

#### Info sharing and public-private sector trust critical to solve impact

Jason Smith, 2-22-2022, Jason Smith currently serves as service chair and as assistant professor for security studies at the National War College. He has served as a leader and aviator in the US Coast Guard and the US Army, as advisor to the commandant of the Coast Guard, as senior policy advisor in the US Senate, and on the staff of the National Security Council. "Forget a Whole-of-Government Cybersecurity Strategy—It’s Time for a Whole-of-Nation Approach," Modern War Institute, <https://mwi.usma.edu/forget-a-whole-of-government-cybersecurity-strategy-its-time-for-a-whole-of-nation-approach/> //jsam

Defensive Public-Private Cybersecurity Partnerships

**Given the limitations inherent to engaging the private sector in offensive cyber operations, defensive options** ought to be more carefully **considered**. Like any successful defense, early preparation and **information sharing is critical**. Building robust defenses and communicating information about vulnerabilities, where the enemy is likely to attack, any early indications of an attack, and how to support and reconstitute areas attacked are key to strengthening defensive measures and limiting damage. In 2017, global shipping company Maersk was the victim of a cyberattack that affected its terminals, ports, and ships around the world, costing the company at least $200 million. **Maersk’s willingness to share information allowed the US Coast Guard to warn other companies, focus resources, and limit cost to maritime infrastructure. The cooperation by Maersk is a great example of what is needed, but it is the exception, not the norm.** The administrations of both the Donald Trump and Joe Biden issued **executive orders to address cyber vulnerabilities, but these orders were for federal systems and did not include the private sector, mainly due to strong industry resistance to government regulation. Companies** exhibit a natural **prefer**ence for a strong, **government-led offensive cyber response to deter would-be attackers**, instead of paying for expensive defensive measures. Nevertheless, protecting networks needs to be the first step in a successful competitive strategy, and communicating threats is integral to shoring up cyber defenses. Consequently, **information sharing is crucial to successful public-private cybersecurity partnerships.** A physical attack is easy to observe, and attribution is usually much easier, allowing for a timely and appropriate response by the government. However, for cyberattacks the government is often dependent on third parties to inform them of not only the occurrence, but also the breadth of the attack. **Increasing reporting requirements is one way to help raise awareness and possible attribution, but mandates alone are insufficient.** Currently, there is a hodgepodge of reporting requirements that vary considerably by industry and oversight agency. Recently, there has been a move to standardize reporting requirements, giving the government better visibility and information to decide appropriate actions. This is not without controversy. Many in industry do not want their victimization made public, because it could reduce revenue, as well as investors’ and customers’ confidence. For instance, the 2013 attack on Target exposed forty-one million of its customers’ payment card information and resulted in a substantial drop in revenue, lost customers, and a large settlement agreement. Moreover, many companies do not view reporting as useful due to a perceived lack of leadership, responsiveness, and assistance provided by the government in response to cyber incidents. Although companies are reticent to provide this information, the government cannot develop a coherent response to these attacks without awareness. There must be coordinated government action that changes incentives and increases trust. Trust, of course, works both ways. **Just as the private sector must trust the government to represent its best interests in responding to cyberattacks, the government must also be able to trust private sector entities in order to effectively partner on cybersecurity**. Engaging private entities on national security interests is not unprecedented. Besides the obvious defense contractors, there are also occasions when private industry is allowed to see behind the curtain. Government must be willing to do this more often. (Admittedly, though, complex ownership and investment structures that often involve non-US persons and financial interests in today’s globalized economy can make this even more challenging.) This goes beyond just setting up additional advisory boards under the Federal Advisory Committee Act. These boards are often just cursory, given little information, and paid little attention to by relevant US government departments and agencies. On the other hand, the boards’ efficacy is limited as they are too often populated with members that have long since retired from industry and no longer occupy influential positions. Instead of building trust between government and industry, they create frustration. Advisory boards need to be populated with current industry leaders and trusted with information and decisions. The government needs to show the private sector how it is part of the nation’s strategic competition with its adversaries.

### S - Russia

#### The CP is key to deterring Russian cyber attacks

Huggins ’22 (Katherine Huggins – Reporter, Medill News Service. “U.S. lawmakers hope to bolster infrastructure's cyber defenses amid Russian threat.” UPI. 4/6/22. https://www.upi.com/Top\_News/US/2022/04/06/Russian-hackers-Senate-committee-hearings/3571649273861/)

Top federal cybersecurity officials and members of Congress said this week that the invasion of Ukraine increases the risk of Russian hackers targeting critical infrastructure, and they urged more coordination between the government and private companies to combat the threat. The United States "desperately needs to revamp the playbook it uses for critical infrastructure cybersecurity," Rep. Yvette Clark, D-N.Y., chairwoman of the House Homeland Security committee's Cybersecurity, Infrastructure Protection and Security Technologies subcommittee, said Wednesday. "Our nation's critical infrastructure is vulnerable to cyberattacks, and the federal government has resources it can bring to bear in closing security gaps, but we've been reluctant to make the private sector come to the table," she said. Subcommittee members on Wednesday heard from experts who outlined how the United States could work to strengthen public-private partnerships in the cybersecurity sector. On Tuesday, the full House Homeland Security Committee discussed securing critical infrastructure against Russian cyber threats. That committee's vice chair, Ritchie Torres, D-N.Y., said that as the United States continues to impose sanctions on Russia and its leaders over its invasion of Ukraine, "we must consider the potential risk to the homeland." "Over the past decade, Russia has demonstrated its ability and willingness to use cyber tools to advance its global agenda. It has used its neighbors in Eastern Europe as testbeds for deploying its cyber capabilities to interfere with elections, spread disinformation, and disrupt critical infrastructure," Torres said. He cited Russia's [attacks on Ukraine's power grid](https://www.bbc.com/news/technology-38573074) in 2015 and 2016 and the [NotPetya attack](https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html) in 2017, which wiped computer data from Ukrainian banks, energy firms, government officials and an airport. For several lawmakers, the question is not whether Russia will orchestrate a cyberattack, but what it will target and when. "I am very worried. I think it's more likely than not that Russia will start using cyber attacks against the West," Rep. [Bill Foster](https://www.upi.com/topic/Bill_Foster/), D-Ill., said in a March interview. "And when that happens, we have to understand how we're going to avoid a retaliatory spiral." A Russian cyberattack most likely would come in the form of ransomware, as SWIFT sanctions have encouraged a reliance on cryptocurrency to access foreign capital, according to Adam Levin, former director of the New Jersey Division of Consumer Affairs and host of the "What the Hack with Adam Levin" podcast. SWIFT is is a Belgian cooperative society that provide services related to the execution of financial transactions and payments between banks worldwide. "Because of all of the sanctions, ransomware becomes a very big deal for [Russia], because it can actually help them by way of cryptocurrency make up some of what they're losing by all the sanctions," Levin said in an interview. The top Republican on the subcommittee, Rep. Andrew Garbarino of New York, said that "cyberthreats posed by foreign adversaries are only becoming more potent." "Potential for malicious Russian cyber activity, as well attacks by other adversarial nations like China, Iran and [North Korea](https://www.upi.com/topic/North_Korea/), is only increasing," he said, calling on Congress to continue facilitating public-private partnerships to curb threats. Specifically, concerns about water infrastructure being targeted have grown since the cyber attack on a treatment facility in Oldsmar, Fla., last February, Levin said. According to investigators, the hacker used remote access software to raise the levels of sodium hydroxide -- a chemical compound used in small amounts to remove metals from water -- from about 100 parts per million to more than 11,000 ppm. An employee noticed something was wrong before anyone was hurt. The Oldsmar hack was mentioned in both hearings, but Rep. Jeff Van Drew, R-N.J., brought up a separate instance of water infrastructure being targeted through a ransomware attack in [Atlantic County, N.J.](https://pressofatlanticcity.com/news/local/cyber-incident-brings-down-acua-website/article_a8432eeb-ce75-54b5-86d9-2a7d1e8bac7f.html) (A similar attack also occurred in [Jersey City](https://www.nj.com/hudson/2021/01/3-months-after-cyberattack-that-threatened-public-health-crisis-jersey-city-mua-computer-systems-still-not-fully-restored.html).) "Services like utility authorities are vital to day-to-day life, and it is imperative that Congress and the administration continue to invest in protecting critical infrastructure everywhere small or large in every way," Van Drew said. "It affects every aspect of our life." While water facilities remain a top potential target, communication infrastructure and financial infrastructure also could be hit, Levin said. "What if they attacked the ability of financial institutions to provide cash through ATM machines?" he said. "Or what if they were to do something that would disrupt the free flow of credit card transactions?" The Cybersecurity and Infrastructure Security Agency was repeatedly mentioned in both hearings as a conduit for combating cyber threats across sectors by increasing information sharing and coordination across private industry and the federal government. "I can't say enough how encouraging it is to see that CISA is developing those really trusted and treasured partnerships in the private sector," said New York Rep. John Katko, the top Republican on the full committee. "It's so critical to their mission and the more we develop that trust and the trusted exchange of information, by far we are going to make the whole cyber landscape safer." Crowdstrike's senior vice president for intelligence credited CISA's Joint Cyber Defense Collaborative for "disrupt[ing] Russian infrastructure preparing for cyber operations." Based in Austin, Texas, Crowdstrike provides cloud workload and endpoint security, threat intelligence and cyberattack response services. "We actively participate in public-private partnerships such as CISA's JCDC, through which we have worked with select industry partners to disrupt Russian infrastructure preparing for cyber operations," Adam Meyers said Tuesday. The White House's acting principal deputy national cyber director, Robert Knake, said the biggest asset the federal government can provide to private sector companies to curb cyber threats is increased intelligence. "We've heard from every private sector company we've talked to is to make sure we provide the one thing private companies can't do on their own, which is intelligence," he said. "Only the U.S. government can collect intelligence and only the U.S. government can provide it back." Lawmakers from both parties appeared motivated to strengthen infrastructure security by improving coordination between the government and private sector to reduce cyber threats, in part evidenced by the passage of the Fiscal Year 2022 Omnibus, which included the Cyber Incident Reporting for Critical Infrastructure Act. The legislation, deemed a "game-changer" in a [statement by CISA](https://www.cisa.gov/news/2022/03/11/statement-cisa-director-easterly-passage-cyber-incident-reporting-legislation), set two new reporting obligations and timeframes for critical infrastructure operators. The agency expressed gratitude for receiving an "unprecedented level of funding."

#### Public-private collaboration is key to countering Russia’s cyber attacks

Fort Mead ’18 (“Russian attack on U.S. election highlights need for public-private cyber security efforts.” *Fort Meade Alliance.* Feb 2018. https://www.ftmeadealliance.org/2018/02/russian-attack-on-u-s-election-highlights-need-for-public-private-cyber-security-efforts/)

Reflecting on Russia’s meddling in the 2016 U.S. election, U.S. Senator Ben Cardin said Fort George G. Meade and its tenants – including the National Security Agency (NSA) and U.S. Cyber Command – constitute “our frontline defense to what I think is the greatest threat to America.” Speaking to a gathering of government officials and private sector executives, Cardin stressed the need for heightened public-private collaboration to resist increasingly sophisticated cyber assaults on American democracy. The gathering, organized by the Fort Meade Alliance (FMA), focused on ways to improve America’s cyber defenses and included insights from NSA Executive Director Harry Coker, Jr. and Leidos Chairman and CEO Roger Krone. The 2016 election demonstrated how the Russian government has become highly skilled at using asymmetric tools – including cyber attacks, propaganda and social media bots – to impact other countries, Cardin said. But the election was “just a small part of the overall design that [Russian President Vladimir] Putin has for an all-out assault on democratic institutions” in the U.S., Mexico and Europe,” he said. The Central Intelligence Agency has already warned that Russia will be “extremely active” in the 2018 mid-term elections, Cardin added. The United States faces “a diverse set of national security challenges from a diverse set of adversaries, both state and non-state actors,” Coker said. Furthermore, the technology employed by those adversaries “will continue to grow exponentially,” he said. “One thing I have noted in my decades within national security is there are plenty of very bright adversaries and they are paying attention … so they are a tough challenge.” A report released in January by the Democratic staff of the Senate Foreign Relations Committee detailed two decades of Putin’s attacks on democratic institutions and called for policy changes to protect the 2018 and 2020 elections. The report “is fascinating and terrifying all at the same time,” said Steve Tiller, FMA President. “It emphasizes that the U.S. and its European allies are still extremely vulnerable to cyber attacks and it recommends a commitment to mutual defense both in Europe and the U.S. against state-sponsored cyber attacks through rapid reaction teams, international treaties and other resources.” Tiller asked what can the private sector do to facilitate those defense efforts? “In America, we still have not figured out how the government and the private sector can work together in cyber,” Cardin said. Collaboration is challenged by a “mindset that we can’t just freely share information about cyber threats and vulnerabilities between the public and private sector,” Coker said. “We need to look at things differently.” Public and private sectors, Cardin and Coker said, need to hone methods of sharing cyber threat information that are safe, productive and trusted by the public. Leaders in cyber, both from the public and private sectors, need to increase efforts to develop and employ a highly skilled workforce, Krone said. In addition to supporting relevant courses in schools and universities, and offering internship programs, cyber leaders need to re-examine labor categories for cyber jobs, he said. “We probably don’t have enough categories at the entry level. Most start at five years of experience as an analyst,” Krone said. That requirement makes it difficult to make good use of new college graduates and often results in contractors being “slow to staff” federal projects, Krone said. “We have to take more risk on our people,” Coker said. “Typically, in the public sector we hire on demonstrated performance… We need to take a look at ability to learn and if the individual is in line with the institution’s core values. We lose out on too many good people because we say, you haven’t done X, Y or Z.” The cyber sector, Krone said, could increase its workforce and staff projects faster if it could make greater use of retiring military personnel who have conditional security clearances and can start work while they complete their permanent clearances. Cyber companies could strengthen America’s cyber defenses by focusing more on “the fidelity of information we get through the digital media,” Krone said. “The attacks in the last election really went to that core where we didn’t know if an article was fake news or not. We didn’t know what messages to believe… That really tears apart the fabric of society.” “We really need to get to the point where we are doing information assurance [to prevent cyber attacks] and not forensics and reactions to cyber events,” Krone said. Information-assurance efforts, Cardin said, would counter one of Russia’s primary attack strategies. “Part of Putin’s design is to discredit all news…and [argue] that no elections are totally free,” Cardin said. “We need to work together to restore confidence in our system, in our independent media… We need to build up the institutions that strengthen our democratic country.”

#### Cooperation between the public and private is key to solve infrastructure

Kennis and Zabierek 22(Graham Kennis is an Air Force officer. He focuses on the intersection of technology and national security policy, most recently serving as an intern for the Cyberspace Solarium Commission and for CSC 2.0 at the Foundation for the Defense of Democracies while completing a Master’s in Public Policy at the Harvard Kennedy School. Previously he served as a research assistant with the Belfer Center’s Cyber Project and as an enlisted communications technician in the Air Force. Lauren Zabierek is the executive director of the Cyber Project at Harvard Kennedy School’s Belfer Center and a 2019 graduate of the Kennedy School’s mid-career MPA program. Her work focuses on strategic, national security issues in cybersecurity and technology. She is the co-founder of the online social media movement called [#ShareTheMicInCyber](https://www.sharethemicincyber.com/), which aims to dismantle racism in cyber security and privacy. She is a United States Air Force veteran and, former civilian intelligence analyst with multiple deployments to Afghanistan. She also established and led the public sector customer success team at the cyber security threat intelligence startup, Recorded Future. 6-2-22 “BUILDING A REGIONAL, RIGHT OF BOOM CYBER DEFENSE NETWORK” <https://warontherocks.com/2022/06/building-a-regional-right-of-boom-cyber-defense-network/>) CL

The invasion of Ukraine thrust the Cybersecurity and Infrastructure Security Agency into public consciousness as the nation’s key cyber security risk advisor during a time of heightened risk. Congress recently passed legislation requiring critical infrastructure operators to notify the agency of security breaches, bringing it into closer contact with the private sector. This development builds on positive momentum for the agency, following a series of executive orders that expanded its authority and created **a specific**[**Joint Cyber Defense Collaborative**](https://www.cisa.gov/jcdc) to share information about threats between the public and private sectors. Nearly four years after its creation, the agency **now has more visibility into the risks the country is facing and more resources at its disposal to combat them. But to capitalize on this momentum toward greater public-private partnership, the agency should deepen its engagement with smaller organizations** in the private sector and at the state and local levels. In our [research](https://www.belfercenter.org/publication/toward-collaborative-cyber-defense-and-enhanced-threat-intelligence-structure), many private sector stakeholders described difficulties working with the federal government on cyber security issues: They didn’t know whom to speak with, and, even when they had a point of contact, did not always get the results they hoped for. What’s more, they sometimes worried about sharing information with federal law enforcement that would subject them to liability. The federal government also has concerns of its own. Private companies and state or municipality-run utilities often lack the resources and financial incentives to implement needed cyber security measures. These systemic issues were highlighted in a recent three-hour phone call between senior Cybersecurity and Infrastructure Security Agency officials and over 13,000 private-sector cyber security professionals. Both agency director Jen Easterly and the stakeholders on the call [noted](https://www.washingtonpost.com/politics/2022/03/28/public-gets-peek-into-tensions-between-us-cyber-officials-industry/?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202) the urgent need to better work with local and regional partners. And while the Joint Cyber Defense Collaborative is bringing the largest companies together with Cybersecurity and Infrastructure Security Agency, it is still only virtual collaboration. In short, there is still a degree of distrust and distance preventing the government and private sector from working together to defend America’s cyber infrastructure. To overcome this, we recommend a more regional focus. The agency should start by bolstering its 10 existing regional offices with the $8 million in funding recommended for the agency’s FY2023 budget. This would bring more capabilities and presence into the field to build trusted relationships, increase information sharing, and focus on right of boom, or post-disaster, mitigation efforts. **Enhancing the agency’s** [**regional offices**](https://www.belfercenter.org/publication/toward-collaborative-cyber-defense-and-enhanced-threat-intelligence-structure#toc-2-0-0) would **capitalize on** its **current momentum** and bring it closer to the end user. To do this, the agency should **transform its** [**regional offices**](https://www.cisa.gov/cisa-regions) from advisory posts **to collaborative** defensive and analysis **centers**. As former commander of Joint Special Operations Gen. (ret.) Stanley McChrystal has [said](https://foreignpolicy.com/2011/02/21/it-takes-a-network/), “It takes a network to defeat a network.” The physical network infrastructure exists in the form of regional offices — with added support from the Federal Bureau of Investigation’s field offices. But those offices could be bolstered by creating additional private and public sector capacity to work alongside the current cadre of cyber security advisors, physical security advisors, emergency communications coordinators, and chemical security inspectors. Borrowing some concepts from the [U.S. military’s Joint Operations Centers](https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/jtf_hq_org_fp.pdf), **these** collaborative defense and analysis centers **could bring together cross-functional teams of analysts** and operators **from the public and private sectors**. These would include representatives from federal regulatory and law enforcement agencies, critical infrastructure sectors, major municipal regions, businesses with cyber defense capability, and [Information Sharing and Analysis Centers,](https://www.nationalisacs.org/about-isacs) which serve to share threat intelligence in specific sectors. We also recommended hosting regular “operations and intelligence” briefings that would hold all these nodes in place. While asking people to physically sit together may seem archaic in the age of COVID, ultimately, we believe that **such a model would bring greater unity, physical breadth, and functional diversity**. They would also make the field office a more accessible touchpoint for businesses and state governments operating within their region. Enabling the Cybersecurity and Infrastructure Security Agency to pour more resources into those offices and bring more participants would boost visibility, sustainability, and scale across the country. It would also combat local threats and build deeper trust by improving information sharing with local businesses and the general population. This can help address the challenges facing smaller utilities like [municipal water systems](https://www.belfercenter.org/publication/its-time-regulate-water-and-wastewater-cybersecurity-heres-how), which have struggled to secure their networks. And **there are resources to do this**. The congressional commissioners who served on t**he** [**Cyber Solarium Commission**](https://www.solarium.gov/home) **recommended $8 million** in additional funding for regional offices in the agency’s 2023 budget. The former executive director of the commission, Mark Montgomery, recently told us that “in locations that are home to a high density of critical infrastructure, a single coordinator will be insufficient to meet the requirements to provide a more mature risk analysis and measurements capability outside of the federal network and provide an increased ability to support special projects and national level events.” The Australian Example Deep, institutionalized regional engagement between the U.S. government and private sector on cyber security would constitute a significant new development. Australia’s network of [Joint Cyber Security Centres](https://www.cyber.gov.au/acsc/view-all-content/programs/joint-cyber-security-centres) provides one good model to emulate. Established in 2017 and located in hubs like Adelaide, Brisbane, Melbourne, Perth, and Sydney, these have succeeded in embedding resources at the local level and building expertise for public-private collaboration. Run by Australia’s Cybersecurity Directorate, the Joint Cyber Security Centres “bring together businesses and the research community, along with state, territory and Australian Government agencies, in an open and cooperative environment” to drive collaboration and information-sharing. Since their establishment, the centers have worked to build trust and better relationships between the government and private sector by offering access to sensitive information and facilitating more rapid and effective responses to cyber threats. Additionally, in order to provide threat intelligence calibrated to an organization’s capabilities and requirements, the centers offered tiered security clearance programs which allow varying levels of access to information and facilities. Right of Boom Enhanced regional offices similar to the Joint Cybersecurity Centres can be particularly valuable in disaster planning and response. As Juliette Kayyem writes in her [book](https://juliettekayyem.com/the-devil-never-sleeps/), The Devil Never Sleeps, we must focus on “left of boom” and “right of boom” planning. The Joint Cybersecurity Centres focus on the left of boom, that is, staving off attacks by raising our collective level of security and implementing cyber security standards through regulations. But, as Kayyem notes, disasters will happen, again and again — like many of us [warned](https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict?utm_campaign=hbr&utm_medium=social&utm_source=twitter) U.S. businesses in the lead-up to and during the Russian war in Ukraine. So we should also focus on mitigating the worst of the disaster’s effect after it happens to make it less severe. Strengthened Cybersecurity and Infrastructure Security Agency regional offices, therefore, could build on the Australian model to support planning for the right of boom. One of the most important aspects of disaster continuity planning is the establishment and maintenance of personal relationships, especially face-to-face ones. Under [Presidential Policy Directive 41](https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident), the Department of Homeland Security is tasked with coordinating the government’s “Asset Response” leg of the Cybersecurity National Action Plan, which involves assessing risk and providing guidance for recovery and damage mitigation. The best way to do this is at the local level, with easily accessible offices that invite companies and organizations to come in and meet and speak with their government counterparts regularly. While some states are working on [Continuity of Economy](https://www.fdd.org/analysis/2022/01/21/lawmakers-plan-continuity-of-the-economy/) plans, disaster recovery is far too important of a national priority for this patchwork approach. The 2021 National Defense Appropriations Act [stipulated](https://www.fdd.org/analysis/2022/01/21/lawmakers-plan-continuity-of-the-economy/) the president must create a plan to address this within two years — and the bipartisan Infrastructure Investment and Jobs Act [appropriated](https://www.fedscoop.com/senate-infrastructure-bill-cyber/) $20 million for the Cyber Response and Recovery Fund to be used during a significant cyber incident. With money, authority, and vision the United States has a real opportunity move the needle on cyber resiliency. An effective plan should bring the states and their homeland security and emergency management offices together with the federal Department of Homeland Security. It should also involve funding, regular exercise at a regional and national level, and the collection of lessons learned. Building out the regional offices would be powerful because at the regional level, there is intimate knowledge of business, critical infrastructure, and the general risk landscape. But it requires even more people, money, and systems connectivity, as well as a mechanism for regular situational awareness. Trust Is Key Going out to the where its customers are located would dramatically expand the Cybersecurity and Infrastructure Security Agency’s effectiveness. Additional representatives — leaders, analysts, and advisors — should be embedded at the local levels to build relationships, broker trust, and ensure that businesses that participate in public private partnerships see a return on their investment. For the system to work, **regional offices should bring in cybersecurity analysts and operators from surrounding state and local governments and members of the private sector to create mission-driven teams with their own esprit de corps**. They should give non-federal entities seats at the table as equals and better access to government leaders and timely intelligence. Teams that know and trust each other will have an easier time sharing intelligence and responding to incidents together. Right now, collaboration isn’t happening at the scale the country requires because the structures are simply not in place. Build the structures and the culture, unify the effort, and results will follow. While the Cybersecurity and Infrastructure Security Agency’s **recent outreach efforts have elevated public awareness of available resources, there still remains work to be done in ensuring that America has timely access to the necessary federal resources in the case of a cyberattack.** As former agency director Chris Krebs [noted](https://www.belfercenter.org/publication/toward-collaborative-cyber-defense-and-enhanced-threat-intelligence-structure), “the future of CISA is in the field.” To defend the networks on which the country relies and recover quickly from inevitable attacks, America needs nodes that can aggregate and share threat information and promote effective responses at the local and regional levels.

### AT - Perm

#### US international cooperation prevents proper preparedness for China

Lee 21 [Eunwoo Lee. "A Networked, High-Tech Alliance Makes an Attractive Target for Cyberattacks". 12-9-2021. The Diplomat. https://thediplomat.com/2021/12/a-networked-high-tech-alliance-makes-an-attractive-target-for-cyberattacks/. 7-3-2022.] -AL

Aware of the “strategic atrophy” induced by information and cyber warfare, particularly by China and Russia, the U.S. Army proffered the concept of multi-domain operations, to include cyberspace as one of its defining arenas. It outlines measures to beef up the integration of technologies and cyber domains with its allies. The U.S. army chief of staff envisages enhanced “military-to-military exchanges,” further “intelligence sharing” and more overseas exercises, and mutual procurement of services among allies. The AUKUS deal, a defense pact to ramp up the exchange of nuclear and cyber technology between Australia, the U.K., and the U.S., and the Quad alliance intended to contain China are the most recent trendsetters. Regardless of the necessity of presenting a unified resolve, however, more integrated alliances will multiply access points for hackers to tap into the collective pool of security in the absence of robust cybersecurity postures among all the parties involved. Despite the tech pomp, Kim Won-jong, an AI researcher at the Korea Army Research Center for Future and Innovation, observes that “their timeline for AI application outpaces adequate cyber defense.” In addition, the allies’ haphazard distribution of intelligence and technology, along with inept cyber defenses, augur ill. The consequences can be dire. “Once the adversaries successfully hack our AI systems,” Kim continues, “they control our modus operandi however they want by injecting their own commands into our machinery.” Under those circumstances, system failure is the best-case scenario, while a “reversal between control and subjection” means bedlam. Yet cooperation to secure cutting-edge technologies has lagged behind the development of these systems. Even with the increasing level of research and intelligence exchange between South Korea and the United States, the first-ever Cyber Cooperation Working group will convene as of 2022. Although state direction and the sheer volume of research outputs do not necessarily guarantee quality and creativity, developments in military cyberspace paint a picture of China as a real cyber threat. Enshrined as one of China’s main strategic priorities, technology espionage through hacking offers “a cheaper and easier path to threatening America’s sources of military power.” China employs machine learning and AI algorithms to replicate a defense model of the target, quarrying the ideal attack sequence and rehearsing optimized forms of hacking. Then, it parlays the information gained through the cyberattack into military capabilities. Conversely, “there has not yet been a uniform effort to integrate AI assurance across the entire U.S. national security enterprise,” according to a report by the National Security Commission on Artificial Intelligence. In October 2021, Nicolas Chaillan resigned from his post as chief software officer for the U.S. Department of Defense, citing the “technology stale” approach that plagues the United States’ cyber defense. “Outdated” bureaucratic principles deprive the workforce of its capacity to leverage “diversity of options.” His desire to upend a work environment where DOD employees are “unempowered to fix basic IT issues” jives with the call from In Jun-beom for cybersecurity forces to be allowed to think outside the box and make breakthroughs in their country’s defense paradigm. Considering the bullish Chinese assertion of its cyber capability and the incompetence of technology “laggards” on the U.S. part, Chaillan remarks that the U.S. and its allies “will have no chance competing” against China unless it adopts a culture of “agility, rapid prototyping and innovation.” As NSCAI puts it in its sobering assessment, “the U.S. government is not prepared to defend the United States in the coming artificial intelligence (AI) era.”

#### Us needs to Focus on technological innovation to counter China – Private Sector Can Help

Ford and Goldgeier 21 Lindsey W. Ford was a David M. Rubenstein Fellow in the Foreign Policy program. She was also an adjunct lecturer at the George Washington University’s Elliott School of International Affairs. Her research focused on U.S. defense strategy in the Asia-Pacific region, including U.S. security alliances, military posture, and regional security architecture. Ford was a frequent commentator on Asian security and defense issues and her analysis has been featured by outlets including the New York Times, the Wall St. Journal, the Financial Times, Politico, Foreign Policy, the Straits Times, CNN, MSNBC, and Bloomberg. “Retooling America’s alliances to manage the China challenge,” Brookings, January 25, 2021, https://www.brookings.edu/research/retooling-americas-alliances-to-manage-the-china-challenge/

Revitalizing the U.S. alliance system will also require operational innovation. Despite talk of creating an “Indo-Pacific Charter” or transforming the Quadrilateral Security Dialogue or “Quad” (which includes the U.S., Australia, Japan, and India) into a formal alliance, such musings are little more than a pipe dream. It is neither practical nor useful to imagine variations on a NATO model for the Pacific. However, deterring China must be understood as a multilateral task that will require the collective capacity of the U.S. and key allies in both Europe and Asia. They will also need to adopt a broader understanding of collective defense, addressing deterrence requirements across a continuum that includes new sub-conventional and non-kinetic threats alongside conventional military challenges. There may be lessons learned from the NATO context that could provide insight into how best to build new operational models more suited to the Indo-Pacific. This could include multi-national staff colleges akin to the NATO Defense College to foster exchanges on joint doctrine and strategic planning, or an expanded use of allied liaisons within national defense institutions or command structures. It could include multi-national training centers that allow allies to engage in high-end deterrence exercises, or international logistics hubs similar to NATO’s Strategic Airlift Capability (SAC) in Hungary. In these and other areas, there are opportunities to build coalition capability in the Pacific that adapt NATO functions without replicating its form. Beyond building collective capacity to operate more seamlessly in response to today’s crises, the U.S. must also think more closely about building alliance innovation ecosystems for the future. With China set to overtake the U.S. in research and development spending — it already spends more on R&D than Japan, Germany, and South Korea combined — the U.S. and its allies will need to treat defense innovation as a combined task. Rising techno-nationalism and the lack of allied innovation networks will make this difficult absent intentional policy leadership. Looking forward, Washington should further expand new bureaucratic mechanisms such as allied R&D pools or defense innovation hubs that could better harness emerging technologies being developed across allied capitals. While the Defense Department is focused on initiatives that will improve America’s sclerotic acquisition and innovation processes, these efforts need an alliance-centric approach from inception, rather than treating allies as an add-on to existing American plans. NATO, for example, might consider establishing an allied version of the Defense Advanced Research Projects Agency (DARPA), in which key allies could collaborate on emerging technologies, as proposed by the 2017 GLOBSEC NATO Adaptation Initiative. Indo-Pacific allies such as Australia, Japan, and South Korea could be incorporated in this initiative through their role as NATO “global partners.”

## NB - Russia

#### NATO stretched too thin - should focus on Russia and terror instead

Ford and Goldgeier 21 Lindsey W. Ford was a David M. Rubenstein Fellow in the Foreign Policy program. She was also an adjunct lecturer at the George Washington University’s Elliott School of International Affairs. Her research focused on U.S. defense strategy in the Asia-Pacific region, including U.S. security alliances, military posture, and regional security architecture. Ford was a frequent commentator on Asian security and defense issues and her analysis has been featured by outlets including the New York Times, the Wall St. Journal, the Financial Times, Politico, Foreign Policy, the Straits Times, CNN, MSNBC, and Bloomberg. “Retooling America’s alliances to manage the China challenge,” Brookings, January 25, 2021, https://www.brookings.edu/research/retooling-americas-alliances-to-manage-the-china-challenge/

As the United States and its allies explore the best way to meet the China challenge, they will need to grapple with three existential questions: Does NATO have a role to play in dealing with China? Because no other military institution provides the same degree of multinational interoperability and capacity, NATO has become a first responder on the global stage many times since the end of the Cold War: delivering humanitarian and medical assistance after the 2004 Indonesian tsunami and during the current COVID-19 pandemic; conducting counterterrorism operations in the Mediterranean and counterpiracy operations in the Indian Ocean; using military force to protect civilian populations in the Balkans in the 1990s and in Libya in 2011; overseeing post-conflict stabilization and reconstruction activities in Afghanistan; and deterring Russian aggression against Eastern Europe. The plethora of missions is in large part due to the lack of alternatives globally. It has also led to concerns, however, that **NATO is stretched too thin.** China has now been added to the alliance’s ever-expanding agenda, providing a surprising point of agreement in an otherwise contentious December 2019 NATO summit, at which NATO members committed the alliance for the first time to deal with China’s “growing influence and international policies.” In April 2020, NATO Secretary General Jens Stoltenberg charged an independent “Reflection Group” with preparing a report eyeing the future; released in November, the “NATO 2030” document put the challenge in stark terms: “China is… best understood as a full-spectrum systemic rival, rather than a purely economic player or an only Asia-focused security actor.” Obvious questions remain about the precise role NATO should play vis-à-vis China. There are certainly a host of global security concerns — ranging from China’s presence in Africa and South Asia to its influence in space and cyberspace — where NATO coordination would be valuable. It is unclear, however, what role NATO could, or would, play in an Asian military crisis with Beijing. NATO allies have limited military capabilities they could bring to bear in the Pacific, and few European partners would be eager to be pulled into a conflict in places like Taiwan or the South China Sea. Given that Article V of the 1949 Washington Treaty refers to “an armed attack against one or more [NATO members] in Europe or North America,” a **Pacific** conflict, even involving U.S. forces, would technically **fall outside NATO’s scope**. But in a spiralling crisis that would implicate Europe’s strategic and economic interests, could NATO afford to remain on the sidelines? At a minimum, Europe could play a valuable role in the political, economic, or even cyberspace arenas. As European allies seek a bigger role in the Indo-Pacific, the U.S. needs to engage them in more frank discussions about these types of scenarios, creating clearer expectations about how different parties might respond before any such conflict appears on the horizon, rather than after one has erupted. Beyond the question of NATO’s role in Asia, there are also tradeoffs associated with European partners seeking a more prominent role in the Indo-Pacific. Encouraging more regular European military deployments to the Indo-Pacific, while they would be welcomed in Asia, could **detract from NATO’s focus** on Eastern Europe to **deter Russian aggression** or in the Middle East to engage in **counterterrorism missions**. These are areas where Europeans will need to shoulder more of the burden in the coming years as the U.S. continues to rebalance its foreign policy to Asia.

## NB – China

### CP Key

#### CP is crucial to surpassing China in AI.

Irwin 21 (Lucas Irwin. Sophomore at Princeton, majoring in Computer Science with minors in Public Life and Statistics and Machine Learning. “One Thousand and One Talents: The Race for A.I. Dominance.” Just Security. April 7, 2021. https://www.justsecurity.org/75474/one-thousand-and-one-talents-the-race-for-a-i-dominance/)

R&D = research and development

In order to improve U.S. A.I. policy, it is vital that the Biden administration understands two points. First, **greater R&D spending** is **necessary to ensure that the United States can keep up with China on A.**I. For the most part, the new administration has embraced this: Biden’s campaign [reiterated](https://fortune.com/2020/11/10/biden-harris-administation-artificial-intelligence/) former Google CEO Eric Schmidt’s assertion that the United States must boost tech R&D because “China is on track to surpass the U.S. in R&D.” It even went on to claim that China’s main reason for investing in new technologies was to “overtake American technological primacy and dominate future industries.” Second, because American allies are themselves investing heavily into A.I., **it is prudent to adopt multilateral solutions which leverage the United States’ historic alliances as opposed to unilateral “America first” responses.** For instance, Germany’s “A.I. Made in Germany” plan has [allocated](https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/ai-investment-by-country.html#endnote-17) €3 billion to A.I. research over the next five years, while France’s “A.I. for Humanity” initiative has injected €1.5 billion into the sector. To balance against China’s advancements, the United States should take advantage of these alliances and ensure that global investments go into developing A.I. capabilities across the broader liberal democratic sphere. This second necessity does not appear to have received as much attention from the Biden administration so far. Despite its general recommitment to multilateralism through rejoining the Paris Climate Accord, reprioritizing NATO, and [calling for](https://www.brookings.edu/blog/order-from-chaos/2021/02/19/the-democracy-summit-must-be-paired-with-a-democracy-strategy/) a “Summit for Democracy,” the Biden administration has largely overlooked the idea of multilateral cooperation on A.I. research. To match the Chinese technological challenge, the United States must establish research initiatives alongside its historic allies which will benefit U.S. A.I. development. This will have the effect of protecting U.S. national security long into the future by guaranteeing that the United States retains the edge over China in crucial A.I. innovations. At the center of this policy should be an upgraded equivalent of China’s “thousand talents” scheme that would be run as a joint initiative between America and its allies. The European Union, United Kingdom, Australia, and Japan’s determination to invest heavily into A.I., paired with their historic ties to the United States, suggests potential for large-scale multilateral research collaboration led by the United States. The Biden administration should therefore suggest the foundation of a multilateral research program—call it “One Thousand and One Talents”—with the aim of attracting the best A.I. specialists from around the globe. Participating governments would funnel their annual A.I. budgets into the scheme in order to fund research projects with important military and commercial applications. The program would ensure that salaries would be directly competitive with China’s “thousand talents” program and that incentives would be put in place to make the Western alternative more attractive than the Chinese one. Like NATO, U.S. leadership would be justified by its status as the main benefactor of the scheme. **The emphasis on multilateralism as a response to U.S.-Chinese competition should come as no surprise**. As Princeton professor John Ikenberry [writes](https://www.foreignaffairs.com/articles/asia/2008-01-01/rise-china-and-future-west), the key thing for U.S. leaders to remember when dealing with China is that “it may be possible for China to overtake the United States alone, but it is **much less likely that China will ever manage to overtake the Western order**.” It is no different with A.I. The new technological challenges facing America call for a far-sighted and judicious foreign policy worthy of the world’s greatest superpower. While China may have the advantages of unrestricted State investment and well-planned incentive programs, it [lacks alliances](https://www.washingtonpost.com/posteverything/wp/2014/07/08/5-reasons-china-has-no-friends/) that run as deep as the NATO friendships the United States has long depended on. To overcome current Chinese advancements in A.I., the **United States** must **unite with its partners** around the world in order to **increase the talent, funding, and skill available** to it. The proposed “Thousand And One Talents” research scheme would boost the United States’ competitiveness vis-a-vis China by pooling the resources of some of the wealthiest and most technologically advanced nations into U.S.-led A.I. development. Given the inevitability of China’s rise, multilateral cooperation with like-minded democracies is the only way of ensuring that the U.S. does not face an existential security threat in the future. The Biden administration must rise to the challenge by uniting with U.S. allies to compete with China on A.I. It is too risky to go it alone.

#### Public-Private coop is only way to deter China

Yuka Koshino, 2022. YUKA KOSHINO is a Research Fellow with the International Institute for Strategic Studies (IISS). Published in January 2022, “2” from “Meeting China’s Military Challenge: Collective Responses of U.S. Allies,” NBR Special Report 96, <https://www.nbr.org/publication/chinas-military-modernization-in-space-and-cyber-and-the-implications-for-the-u-s-japan-alliance/> //jsam

**Economic-Security Level Encourage public-private cooperation in order to maintain superiority in technology with dualuse implications in the cyber and space domains.** The U.S.-Japan **summit** joint statement—which included science-and-technology cooperation in areas such as 6G, AI, quantum information and technology, and civilian space programs—**is an important step in maintaining technological superiority over China in the cyber and space domains.** The Quad’s working group on emerging and critical technology creates further opportunities for public-private cooperation between like-minded regional countries. The United States and Japan could also consider expanding technology partnerships with other like-minded technology powers, such as the United Kingdom, France, Germany, South Korea, and Taiwan. Invite Japanese firms to partner with U.S.-based nonprofits that share real-time information on trends in cyberdefense. Inadequate network-security levels among Japanese defense contractors and commercial companies undermine private-sector cooperation between U.S. and Japanese defense and civilian technology firms. To prevent espionage and technology outflow to China, Washington could encourage U.S. industrial consortiums and nonprofits with capabilities for real-time information sharing on cyber incidents to partner with Japanese private companies and thereby boost their cyberdefense capabilities.

#### The US needs to focus on itself to combat China - Distance from NATO promotes European self-reliance and strength

Ford and Goldgeier 21 Lindsey W. Ford was a David M. Rubenstein Fellow in the Foreign Policy program. She was also an adjunct lecturer at the George Washington University’s Elliott School of International Affairs. Her research focused on U.S. defense strategy in the Asia-Pacific region, including U.S. security alliances, military posture, and regional security architecture. Ford was a frequent commentator on Asian security and defense issues and her analysis has been featured by outlets including the New York Times, the Wall St. Journal, the Financial Times, Politico, Foreign Policy, the Straits Times, CNN, MSNBC, and Bloomberg. “Retooling America’s alliances to manage the China challenge,” Brookings, January 25, 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.

### China Leading Now

#### American hegemony is dependent on wire-thin margins of error in tech; China poised and ready to surpass in AI

Javers 21 (Eamon Javers, Eamon is the Senior Washington Correspondent for CNBC, OCT 22 2021, “America must protect these 5 technologies if it wants to remain a superpower, intelligence officials warn,” CNBC, https://www.cnbc.com/2021/10/22/america-must-protect-5-crucial-technologies-to-remain-superpower-officials-warn.html)

WASHINGTON – U.S. intelligence officials have issued a stark warning: **America’s status as a global superpower depends on maintaining a lead in five key tech**nologies – and America’s **rivals are trying to steal every one of them**. Officials said they are concerned that **foreign theft** of American technologies **could** not only **rob the U**nited **S**tates **of econ**omic **leadership** in the key sectors, but could **threaten the country’s ability to** even **remain active in the industries** at all. The five technologies identified by intelligence officials are:**A**rtificial **i**ntelligence Quantum computing **Bioscience** Semiconductors **Autonomous systems** Officials cited legal and illegal activities, particularly those conducted by China, that have crippled competitiveness in sectors such as steel and solar panels. They also pointed to China’s wipeout of the Australian rail industry as an example. “We don’t want what happened in those other industries to happen here,” said Michael Orlando, acting director of the National Counterintelligence and Security Center, which falls under the Director of National Intelligence. When asked what the impact would be if the U.S. loses supremacy, he said: “It could be severe. We’ve got to focus on these industries because we can’t afford to lose them.” Has the U.S. already lost the AI battle to China? In a new report, the NCSC wrote that “these sectors produce technologies that may determine whether America remains the world’s leading superpower or is eclipsed by strategic competitors in the next few years.” In each area, officials said, **adversary nations** have **used** a blend of **legal and illegal methods** – ranging from **hiring talent to mergers** and acquisitions **to hacking** and old-fashioned **spycraft** – **to steal and replicate American tech**nology. Over the past several months, officials have briefed a small group of executives and academics on the dangers to their research. Now that the report is public, officials plan on a more aggressive outreach to industry and universities. Officials said many private sector business leaders fail to appreciate that the outreach they get from Chinese and Russian entities for everything from joint ventures and partnerships to mergers and acquisitions is part of a national strategy by those governments to acquire those technologies and replace the American firms that are producing them. **Intel**ligence **agencies fear** that **U.S. firms will** not only **lose their edge**, but will be **entirely pushed out of the tech**nology **sectors** crucial to the 21st century. “Its not just the loss of intellectual property, but the loss of a complete business model” said Edward You, NCSC’s national counterintelligence officer for Emerging and Disruptive Technologies. He said vulnerability is particularly acute in health technology. “Because of our short sightedness, we may wake up one day and discover that we have become health care crack addicts and China has become our pusher.” Their goal is to explain to companies and universities that they are on the receiving end of a sophisticated, and often devious, effort by foreign governments to make off with valuable technology — and that some transactions that appear to be simple business deals are more dangerous to the country. “People are having trouble understanding the bigger picture here and the ways that legal and illegal come together,” Orlando said. Any particular deal could be attractive on the individual merits, but American business leaders should recognize that these offers aren’t coming on the merits. “It wasn’t just because it was a good investment,” he said. “It was because it was part of this larger plan.” Intelligence officials, however, stopped short of recommending “decoupling” the U.S. and Chinese economies or of stopping the flow of students and employees from China and Russia, citing an awareness that collaboration can be mutually beneficial. An overall area of concern is the United States losing its ability to develop and manufacture its own supply chain of biological and health care supplies — a vulnerability that became all too clear during the Covid-19 pandemic and could be even worse during the next one, according to You. “We’re dependent on them,” he said. “They could develop a countermeasure before anybody else does. An effective defense is the equivalent of an offense. They can withhold supply like they did with masks. They have all the strategic advantages.” The report found that **China** “possesses the might, talent and ambition to **potentially surpass the U.S. as the world’s leader in AI in the next decade if current trends do not change.**” Officials cited the 2020 U.S. indictment of two Chinese hackers working with the Chinese Ministry of State Security for their part in a 10-year hacking campaign against a wide range of Western targets, including a UK-based AI firm. Officials also expressed concern about Russia, citing MIT’s 2019 announcement that it would extend its partnership with Russia’s Skolkovo Institute of Science and Technology and the Skolkovo Foundation. MIT said the partnership would focus on “strengthening research collaborations between individual faculty members at the two institutions.” American officials pointed out that the U.S. Treasury Department imposed sanctions on Viktor Vekselberg, who headed the Skolkovo Foundation, in 2018. (The university removed him from its Board of Trustees after the sanctions announcement.) The intelligence community report found that quantum computers — which can, in principle, use the unique properties of atoms and photons to solve certain problems much faster than ordinary computers — will pose national security and economic challenges. “A large scale quantum computer could potentially allow for the decryption of most commonly used cybersecurity protocols, putting at risk the infrastructure protecting today’s economic and national security communications,” the report said. In the race to develop practical quantum computers, the officials said, the winner will have a tremendous strategic advantage. The report noted that foreign competitors are recruiting American experts to advance their own quantum programs. “Whoever acquires a quantum computer can break every encryption system we have here,” said Orlando. “And quantum radars can detect our stealth aircraft and submarines.” Officials were particularly critical of China’s WuXi Biologics, which purchased Bayer’s manufacturing plant in Germany, Pfizer’s manufacturing plant in China and CMAB Biopharma Group in China. The Chinese company is also building manufacturing plants in Massachusetts and Ireland. “We’re building or acquiring manufacturing capacities in Ireland, the U.S., and Germany in response to growing customer demand around the world, which are supported by local government and communities as well,” said Yixin Zhang, the assistant director of corporate communications and public affairs at WuXi Biologics. “Growing customer demand for biologics has required our company, like many others in the industry, to build new facilities and acquire existing ones in various markets.” Another company, the former parent of WuXi Biologics, has announced a plant in Delaware through a subsidiary. Because of WuXi Biologics’ enormous manufacturing capacity, American bioscience companies that produce vaccines and other biotech products may find themselves using Chinese controlled plants by default. “They don’t have to steal our intellectual property anymore,” said You. “If you want to scale manufacturing, we’re dependent on Chinese manufacturing, so we’re going to have to give them the IP [to produce the products].” The fragile nature of the semiconductor supply chain is well known, but the report found that the U.S. is heavily dependent on a single company in Taiwan. It also found that adversaries can get access to the supply chain and put compromised chips in U.S. commercial and defense systems. Officials singled out a wave of Chinese acquisitions in the space, including Chinese private equity firm Wise Road Capital March purchase of South Korea-based MagnaChip for $1.4 billion. The report concluded that autonomous systems also present a potential security threat, by expanding the type of target hackers will be able to go after in the future and by gathering an enormous amount of data on drivers in the Unites States. Officials cited a September report that the Chinese had illegally purchased an Italian-based military drone company in an effort to gather autonomous technology. Officials flagged the 2019 arrest of a former Apple employee who was charged with stealing autonomous vehicle secrets from Apple with plans to pass them to a Chinese competitor.

#### China is winning the AI race – the US can win BUT it’ll require a massive effort

Allison and Schmidt 20 [Allison, Graham. Eric Schmidt “Is China Beating The U.S. To AI Supremacy?". Belfer Center For Science And International Affairs, Date Published: August 2020, https://www.belfercenter.org/publication/china-beating-us-ai-supremacy. Accessed 3 July 2022. Douglas Dillon Professor of Government, Harvard Kennedy School Member of the Board, Belfer Center Former Director, Belfer Center Faculty Affiliate, Future of Diplomacy Project Eric Schmidt is an accomplished technologist, entrepreneur and philanthropist. He is the co-founder of Schmidt Futures, and former CEO & chairman of Google]//DL

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

#### US and China continue AI race, but China leading NOW

 Jack **Kotin**, Ben **Armour, 4-6-2022**, (economist, linguist, and fluent in five languages. He graduated with a Masters in International Economics and Finance, from Brandeis International Business School, and has worked as a market research analyst, project manager, and data analyst for GE, IBM, and Meituan Dianping and lawyer and freelance reporter, editor, and translator) "China, US Break Ahead of the Pack in Race for AI Hegemony," No Publication, <https://www.the-yuan.com/271/China-US-Break-Ahead-of-the-Pack-in-Race-for-AI-Hegemony.html> --MV

BOSTON AND LONDON - The rivalry that has been simmering between China and the United States, the world’s two leaders in developing artificial intelligence (AI) technology, is now nearing the boiling point as the two countries’ lines of battle become drawn ever more clearly in policy documents, white papers, and intelligence bulletins. The US has advantages such as leading hardware, research, and talent, whereas China has unparalleled masses of AI-ready data at its disposal to drive technological development, a strong will to succeed in its quest for primacy, and a head start in its already widespread deployment and adoption of many digital technologies. Since 2017, China has been producing more AI scholarly research than the US. But in 2020, for the first time, China also surpassed it in AI-related journal citations, according to last year’s Stanford University AI Index Report. “Citations measure whether the ideas you’re putting out are novel and have impact - not just that you have a lot of researchers pumping out publications,” said Michael Sellitto, Stanford University Human-Centered Artificial Intelligence deputy director and a member of its AI Index steering committee. “The data suggests that China is making more contributions to basic AI knowledge now, a qualitative improvement,” per the Stanford report. “I don’t think they’ll be number one, because I think there’s still a level of genius and creativity in Silicon Valley that persists and will always persist,” Breyer Capital founder Jim Breyer told CNBC, likening the two superpowers’ AI rivalry to the US-Soviet space race of the 1950s. In June 2020, San Francisco-based independent AI research lab OpenAI announced the launch of its GPT-3, the third generation of its massive Generative Pre-trained Transformer language model, which can write computer code, poetry, and everything in between, various media reported at the time. A year later, with considerably less ballyhoo, Tsinghua University’s Beijing Academy of Artificial Intelligence unveiled an even larger model, Wu Dao 2.0, with 10 times as many parameters - the neural network values that encode information. GPT-3 has 175 billion parameters, whereas Wu Dao 2.0’s creators claim that their model has 1.75 trillion. Not only can it generate text as GPT-3 does, but it can also generate images from text descriptions like OpenAI’s 12-billion parameter DALL-E model. Furthermore, it has a scaling strategy that is similar to Google’s 1.6 trillion-parameter Switch Transformer. Even as AI thus fuels the rivalry between China and the US, it also is driving the two countries far ahead of the rest of the world in innovation, economic growth, and national power, according to the Brookings Institution, a think tank based in Washington, DC. China’s official statements promoting the military-civil fusion of technological development to erode America’s competitive edge also prompt unease, which is further amplified by China’s grand trillion-dollar Belt and Road Initiative (BRI) infrastructure program that spans nearly 140 countries and is central to its plan to extend its global influence. The Digital Silk Road (DSR) is a key component of the BRI and seeks to reach into the digital sphere through the DSR’s main assets - fifth-generation wireless network communications technologies, mega data centers, AI, and satellite navigation systems - all of which have critical ramifications for data privacy, national security, and global cyberspace governance, and which will endow the Chinese with the power to access, analyze, and exploit the data of BRI recipient nations. Some worry this will also enable China to set global technological standards, according to the Brookings Institution. China’s actions have fed what Dean Garfield, president and chief executive of the Information Technology Industry Council, has denoted a new “hysteria” in Washington that America is ceding its innovation edge to China. Apropos of which, ex-Secretary of State Condoleezza Rice also said, “When we see [China]... say, ‘We’re going to do whatever it takes to surpass the United States’... you’re going to get a response from the United States,” per the Brookings report. Much of that response has been seeking to slow or arrest China’s progress by tightened screening of foreign investments in core technologies, scrutinizing academic exchanges, imposing tariffs to reduce China’s competitiveness in key sectors, increasing prosecutions of Chinese for economic espionage, and greater investment in counterintelligence. Arguments for ‘decoupling’ the economic relationship between the US and China by collapsing ICT supply chains would do just that. The US technology sector is deeply intertwined with China’s, with high-level collaboration between researchers and engineers and rising tallies of co-authored academic papers, and joint investments by US and Chinese venture capital firms into AI-related firms in both countries, Brookings said. In AI implementation in the civil sphere, China has greatly outpaced the West, open media platform China-US Focus reported last month. China instituted its Social Credit System in 2014 to monitor ordinary citizens and confer benefits or restrict privileges. The system is run on facial recognition and Big Data analysis powered by AI algorithms. China’s device market is also driving innovation, most notably in smartphones, cameras, robots, wearables, smart speakers, automotive, smart mirrors, and computer processors. With respect to US-China competition in the AI space, many US officials, among them Nicolas Chaillan, ex-chief software officer of the Air Force, fear the US may lose the AI race against China because the US is not funding critical AI projects as aggressively, per the China-US Focus report. In comparison to the more centralized Chinese research and development (R&D), most innovation in the US occurs in the private sector and is not directly aided by the government. This ‘decoupling’ or disconnect often creates delays and information gaps. The US still leads in military AI, but this may soon change as China continues to propel innovation with Big Data, digital surveillance, and cloud computing. The US holds leads in talent, research, development, and hardware, while China surpasses in implementation, as well as data quantity and quality, but in recent years China has succeeded in slowly leapfrogging the US and seems well positioned to overtake it in future. The first country to acquire an AI ‘strategic weapon’ will have a huge advantage in both security and the global economy, per the report. China’s cabinet the State Council announced a bold plan to push its AI sector in 2017, aiming to make the country the world's “major AI innovation center” by 2030. The slew of policies which various government departments have since issued on that basis have now coagulated into the edifice of the nation’s AI governance and support infrastructure.

### AT: Cooperation with China

#### Cooperation with China does not mean that there’s no competition

Allison and Schmidt 20 [Allison, Graham. Eric Schmidt “Is China Beating The U.S. To AI Supremacy?". Belfer Center For Science And International Affairs, Date Published: August 2020, https://www.belfercenter.org/publication/china-beating-us-ai-supremacy. Accessed 3 July 2022. Douglas Dillon Professor of Government, Harvard Kennedy School Member of the Board, Belfer Center Former Director, Belfer Center Faculty Affiliate, Future of Diplomacy Project Eric Schmidt is an accomplished technologist, entrepreneur and philanthropist. He is the co-founder of Schmidt Futures, and former CEO & chairman of Google]//DL

Fifth, while competing vigorously with the intention of sustaining U.S. leadership, we must recognize at the same time the necessity of cooperation in areas where neither the United States nor China can secure its own minimum vital national interests without the help of the other. The consequences of human energy consumption on the climate offers a vivid illustration. If either the United States or China keeps emitting greenhouse gases at the current rate, in one hundred years, this could produce a biosphere in which neither nation can survive. Thus there is no viable alternative to cooperation. The same is true in other realms including preventing third party provocations—for example, in North Korea or Taiwan—from dragging the United States and China into a catastrophic war; and cooperation to prevent recurring financial crises like the Great Recession of 2008 from cascading into another Great Depression. We suspect there may be an analog in limiting the unconstrained advance of AI. **The possibility that nations could simultaneously compete ruthlessly, on the one hand, while cooperating intensely, on the other, sounds to diplomats like a contradiction. In the world of business, however, it is called life**. While no one has yet developed a felicitous term for what is sometimes called “coopetition,” Apple and Samsung offer a powerful example. The two are ruthless rivals in the global market for smartphones (where, in fact, over the past five years Samsung has become number one). But who is Apple’s largest supplier of components for smartphones? Samsung. Managing a relationship that is simultaneously competitive and cooperative requires vigilance, judgment and agility in adapting. But if, as we believe the evidence shows, technologies on a small globe have left the United States and China with two—and only two—options, we believe they can find ways to coexist, however uncomfortably, if their only alternative is mutual destruction.

#### Collaboration fails – too many obstacles

Horowitz and Khan 22 ([Michael C. Horowitz](https://www.cfr.org/bio/michael-c-horowitz-0) and [Lauren Kahn](https://www.cfr.org/expert/lauren-kahn) 22 Why DoD’s New Approach to Data and Artificial Intelligence Should Enhance National Defense," Council on Foreign Relations, 3-3-2022 https://www.cfr.org/blog/why-dods-new-approach-data-and-artificial-intelligence-should-enhance-national-defense) CL

**The ability of the United States to compete in the 21st century depends on U.S. leadership in data and artificial intelligence** (AI). In response, the Department of Defense (DoD) is taking a new and much-needed approach to U.S. defense efforts in data and AI. David Spirk, the departing Chief Data Officer of the Pentagon, [made clear](https://www.fedscoop.com/david-spirk-cdo-departing-dod/) yesterday that the office of the Chief Digital and AI Officer (CDAO), in addition to its other functions, will be [the successor organization for](https://media.defense.gov/2021/Dec/08/2002906075/-1/-1/1/MEMORANDUM-ON-ESTABLISHMENT-OF-THE-CHIEF-DIGITAL-AND-ARTIFICIAL-INTELLIGENCE-OFFICER.PDF) and replace DoD’s [much](https://www.fedscoop.com/jaic-dod-ai-authorities-bob-work/)-[touted](https://breakingdefense.com/2021/03/jaics-lt-gen-groen-if-we-want-ai-to-be-our-future-then-ai-has-to-be-our-present/) Joint Artificial Intelligence Center (JAIC). While the JAIC symbolized DoD’s efforts to get smart on AI beginning in 2018, the integration of data and AI represents a maturation of the U.S. AI approach—one that elevates the importance of AI in national defense. The JAIC itself was not as important as what the JAIC stood for—DoD’s commitment to U.S. defense AI leadership. In paving the way forward and getting AI on the agenda, the JAIC succeeded. From this point on, a more cohesive approach to AI and data through the CDAO is more likely to accelerate AI adoption throughout the U.S. military because it links DoD’s AI efforts with data, the fuel AI requires. For U.S. defense AI adoption, in particular, aligning these organizations could be game-changing. Addressing DoD’s [siloed data](https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/DEPUTY-SECRETARY-OF-DEFENSE-MEMORANDUM.PDF), standardizing and improving its quality and access, is a precondition to having the data necessary to train algorithms for many defense uses, and any future technologies that rely on collecting, processing, and using information. Implementation will be critical and heavily dependent on two things. First, to catalyze AI adoption, **the CDAO will need to develop close relationships with the military services and combatant commands.** Second**, the CDAO will need to coordinate with DoD’s research and development organization**s, such as the Defense Innovation Unit, leading on AI experimentation and research. There is hard work ahead, but the new organizational design is promising. [The office of the CDAO](https://media.defense.gov/2022/Feb/02/2002931807/-1/-1/1/MEMORANDUM-ON-THE-INITIAL-OPERATING-CAPABILITY-OF-THE-CHIEF-DIGITAL-AND-ARTIFICIAL-INTELLIGENCE-OFFICER.PDF) brings together previously independent components of DoD: the JAIC, the office of the Chief Data Officer, the Defense Digital Service (DDS), and the Office of Advancing Analytics (ADVANA). The office of the Chief Data Officer is in charge of data management and coordination, DDS finds digital solutions for internal data and security issues, and ADVANA aggregates data and conducts data analytics. The combination of these offices raised questions about whether an independent JAIC was necessary for U.S. defense AI leadership. Departing CDO Spirk [says that](https://www.fedscoop.com/david-spirk-cdo-departing-dod/) the CDAO will be “taking the best parts of all the organizations it is overseeing and redistributing them for faster and better decision-making.” We agree. At present, not only is DoD’s data siloed but its AI efforts and initiatives are as well. According to the company Govini, in FY21, **fifteen separate departments and organizations funded and worked on AI and AI-adjacent technologies**, often without formal coordination or throughlines. **This has led to redundancies, gaps, inconsistencies in application and access to data and resources,** and an overall hodge-podge of AI efforts. DoD has acknowledged this and is making organizational changes necessary to accelerate AI adoption even more by restructuring its AI approach from the ground up. Now, CDAO will have teams working on policy and governance, technology development, and rolling out data and AI for the Pentagon and the military services, to avoid bureaucratic duplication and confusion that could undermine the CDAO’s overall authority. In particular**, bringing the data and AI teams together will improve the data DoD needs for AI development**. Some might fear that the reorganization of the JAIC’s functions within the CDAO means the United States is not as committed to the role of AI in the future of U.S. national defense. Based on current information, this concern is misplaced. First, the JAIC was created so the U.S. military could effectively take advantage of the way AI will shape the future of war. It succeeded in many ways. Recognition of the importance of AI for the future of U.S. defense, and national security in general, is much more widespread. The JAIC made headway on AI adoption and data literacy, with initiatives like “[AI 101](https://www.fedscoop.com/jaic-piloting-artificial-intelligence-education-for-dod/),” and on the data integration issue, as part of the [Artificial Intelligence and Data Initiative](https://breakingdefense.com/2022/02/jaic-developing-first-of-its-kind-integration-layer-for-ai-algorithms/) (AIDA). The military services are investing more in AI and related technologies such as autonomous systems. This, ironically, makes an independent JAIC less necessary. Second, **the JAIC has also faced challenges** that the CDAO approach can address. The JAIC had multiple missions, **including advising DoD on AI adoption, funding AI research, and building AI tools itself.** The JAIC also lacked the authority to advance military service adoption of AI on its own, or to itself transform the connection between AI and overall DoD policy and strategy. The JAIC ended up arguably not policy-focused enough to lead on policy, and not technically equipped enough to lead on algorithm development. While the JAIC encouraged AI investment within DoD, **its existence also highlighted how the uncoordinated DoD AI portfolio required even more organization**. The CDAO approach will address some of these issues by fusing DoD data and AI efforts, as will a growing focus on AI in other DoD components, from Research & Engineering on the technology development side to OSD-Policy (Office of the Secretary of Defense Policy) on the strategy and governance side. Third, **it is difficult to get things immediately right when it comes to converting emerging technologies into adopted innovations, especially for conservative institutions like** **militaries**. We think about experimentation as a critical part of how the technology invention process works, but the same is true when it comes to transforming organizations. Given the way data access and integration are essential to innovation, consolidating data and AI, rather than having a specific JAIC only focused on AI, will make technological adoption across DoD more likely. While it will hopefully spur AI forward within the department, subsuming the JAIC into the CDAO does come with some risks. Currently, there is a widespread understanding that AI is essential for U.S. success in strategic competition and defense leadership. However, we may be taking the prioritization of AI for granted, and future DoD leaders might have a different perspective even if the capabilities of AI tools continue to mature and advance. If that were to happen, the absence of an independent JAIC could lead to a withering of focus on AI, and a downplaying of its importance and relevance, just at the key moment advances in algorithms become more relevant for many military functions. Reward requires risk, especially when it comes to innovation with emerging technologies like artificial intelligence. Technology development is not a linear process and often [involves failure](https://www.foreignaffairs.com/articles/united-states/2021-04-06/perils-overhyping-artificial-intelligence) along the way. Innovation becomes even more challenging when it requires organizational change to facilitate adoption. Saying goodbye to the JAIC will be bittersweet—the JAIC played a critical role in advancing the U.S. military’s emphasis on AI and set the table for what is next. Moving forward, however, bringing the JAIC into the CDAO will create a more integrated approach to AI and data that is likely to help the United States achieve defense AI leadership.

# Aff Answers

## Perm

### US-NATO Key

US and NATO cooperation is key to counter cyber-threats

Alexander ’12 (David, Correspondent in Jerusalem, New Delhi and London. 20+ years in Washington, with stints at Pentagon, White House, “Global cyber arms race engulfing web – Defense official,” Reuters, April 10, 2012, https://www.reuters.com/article/usa-defense-cyber/global-cyber-arms-race-engulfing-web-defense-official-idUSL2E8FADH320120411)-AT

WASHINGTON, April 10 (Reuters) - A global cyber arms race is engulfing the Internet and the best way to counter the rapidly escalating threat is combining the efforts of U.S. agencies, private firms and international allies, cyber security officials said on Tuesday. Cyber experts from across the U.S. government, speaking at a conference at Georgetown University, said organized crime, espionage and security activity on the Internet pose a rising threat to U.S. intellectual property, military superiority and critical infrastructure. “What we’re looking at is a global cyber arms race,” said Rear Admiral Samuel Cox, director of intelligence at U.S. Cyber Command, which was set up 18 months ago to protect Pentagon computer networks and conduct offensive cyber operations if the president orders them. “It’s not proceeding at a leisurely or even a linear fashion but in fact is accelerating. I wouldn’t claim that it’s following Moore’s law, but the curve looks kind of similar,” he said, referring to a computer industry rule of thumb that computer processing power doubles every couple of years. Howard Schmidt, cyber security coordinator at the White House, said more than $8 trillion worth of transactions were carried over wired and wireless networks each year. “This is not just a national security issue,” he told the conference. “It’s a national security, public safety as well as economic.” Officials said the most effective way to counter the threat is to adopt an approach that promotes collaboration among government agencies and reaches out to private industry as well as international partners. TEAM SPORT. “To really operate effectively in cyberspace ... it’s really a team sport,” said Steven Schleien, the principal director for cyber policy at the Pentagon. That’s why the Defense Department has been working with private companies and allies like NATO, Japan and South Korea to discuss information sharing and coordinated responses to incidents on the Internet, he said. NATO wants to bring all of the civilian and military networks in the organization under the wing of the NATO Computer Incident Response Capability by the end of 2012, which would allow a coordinated response to cyber attacks. The United States has begun discussions on cyber security with Japan, South Korea and New Zealand, and is working closely with the Britain and Australia on a “full spectrum” of cooperation in cyberspace, Schleien said. The United States does not view arms control treaties as a means of dealing with the problem but would like to see the international community agree on norms of behavior for cyberspace, he said. “This is not an area where arms control works. I don’t know what we would monitor. I don’t know how we would verify anything in terms of cyber weapons or cyber tools,” Schleien said. Discussions on norms of behavior would begin to address the issue of how to fight proxies who carry out Internet attacks on behalf of governments, and “hactivists,” who attack computer networks for their own political ends. “How do you deal with hactivists from your soil?” Schleien asked. “Are you responsible as a sovereign nation for what comes out of your country?” The issues are sensitive and complex. A U.S. nonprofit group, for example, concluded Russian civilians acting with advance notice of Russian military intentions carried out cyber attacks in the 2008 Russia-Georgia conflict. Some websites used to organize those attacks were hosted in the United States.

#### NATO using leading members tech is key

**Berger ’21** (Federico Berger, Junior Fellow at NDCF, “The Alliance in the loop: NATO and Artificial Intelligence,” NATO Defense College Foundation. 12/21. <https://www.natofoundation.org/wp-content/uploads/2021/12/NDCF-Paper-Berger-NATO-and-Artificial-Intelligence-151121.pdf>)

In a context where an enhanced AI adoption in the defense sector seems imminent, the NATO Defense College’s paper “NATO-mation” cleary outlines a set of priorities for the Alliance to develop a coherent approach, with some of them that should be at the very heart of the issue. First of all, the Alliance should establish ethical principles around which the development of these systems remains in-line with the founding principles of the transatlantic bond. This would be an opportunity to become a trend-setter in the international arena in an ethical approach towards R&D. Second on the list, NATO Allies should work together to innovate their workforce, as the human side of the process becomes ever more crucial in a highly interactive work environment. A further focus should be given to Hacking for Defense-type initiatives, but also to the support of creative individuals and innovators of the sector. Third, the Alliance needs to develop new concepts and doctrines to establish clearly which fields of AI are more promising and attracts investments from a defense perspective. To this extent, simulations, exercises, and wargames are essential, also to develop common standards, approaches, and priority areas among Allies. The fourth point involves maintaining NATO and Allies’ technological edge over the adversaries. Reinvigorating investments in R&D is the very first condition, but promoting cooperation as well as coordination on investments and reforms must not be forgotten. Finally, the pressing issue of arms control. The Alliance has historically played an important role in deterrence and defence as a forum for discussion, and the field of AI must not be an exception. With the adoption of AI becoming pervasive and the rise of Lethal Autonomous Weapon Systems (LAWS), Allies should pay attention at identifying potential multilateral solutions which preserve international stability. As a matter of fact, the Alliance needs more than ever cohesion and collaboration to face the multiple challenges deriving from technological revolutions. But as Ambassador d’Aboville precisely pointed out in the NDCF Game Changers 2020 Dossier: NATO Defense College Foundation Paper “NATO offers proven consultative mechanisms and a unique network for collaboration on defence and security questions, being a natural platform for collaboration. […] But for such a debate to be productive, one has first to convince the decision makers and the public in the Alliance that these technologies applied to defence have an increasing momentum on their own, and, if we want to redirect it towards our own security interests (or convince others that there is a potential shared interest through arms control), we cannot be complacent or ignore facts. Denying ourselves these capabilities will not stop potential adversaries in pursuing them for their own interests.”

## No Solvency

### CP Fails

#### US law limits private entities from hacking back – have to be cautious with private sectors

Jason Smith, 2-22-2022, Jason Smith currently serves as service chair and as assistant professor for security studies at the National War College. He has served as a leader and aviator in the US Coast Guard and the US Army, as advisor to the commandant of the Coast Guard, as senior policy advisor in the US Senate, and on the staff of the National Security Council. "Forget a Whole-of-Government Cybersecurity Strategy—It’s Time for a Whole-of-Nation Approach," Modern War Institute, <https://mwi.usma.edu/forget-a-whole-of-government-cybersecurity-strategy-its-time-for-a-whole-of-nation-approach/> //jsam

Limitations to Offensive Public-Private Cybersecurity Partnerships

**US law**—specifically, 18 US Code § 1030—**prevents private entities from hacking into another computer system**. Proponents of hack-back policies find this law overly restrictive. Indeed, frustration with current policies has led to action by the government. Congress has introduced several pieces of legislation aimed at loosening restrictions on hacking back. Some advocates have gone even further by proposing modern day letters of marque authorizing certain companies or individuals to act on behalf of the government to disable or disrupt the attacking systems. Moreover, **hacking back is not as simple as it seems and there are good arguments for a cautious approach**. **While proponents of authorizing the private sector to hack back typically also advocate for governmental oversite, it is unclear that the government has the capacity or the expertise to provide it.** Indeed, Jason Healy and Robert Jervis have argued convincingly that US government departments and agencies involved in cybersecurity are rarely even able to maintain awareness of offensive cyber operations conducted by other US government departments and agencies. Additionally, **attribution for cyberattacks is not easy**. The bad guys often originate their attacks from innocent users’ machines they have taken over, employing bots, botnets, or zombies. Disabling or destroying the machines hurts innocent users (they are also victims of the hackers) and not the actual attackers. Imagine the potential harms if an attack was made to appear to have originated from a hospital’s IT network. Hacking back could result in real loss of life. Furthermore, while there is a lot of focus on offense and the ability to strike back, too much offense can create other problems, like instability in international relations. **A back-and-forth exchange of cyberattacks between nation-states can spiral quickly beyond what either nation intended. What started out in the cyber world can escalate into brinkmanship and lethal force.** In short, the United States is right to be cautious with empowering private entities to act offensively on behalf of the government. The past twenty years has demonstrated that the use of private military contractors comes with its own issues. Scandals surrounding Blackwater and other contractors has shown what happens when government allows privatization of inherent government functions.

### NATO Key

#### NATO is key for a unified response.

**Ricart ‘22**, [ Raquel Jorge is Analyst at Elcano Royal Institute working on the technology and digital agenda, she holds a Master’s in Security Policy, with a concentration in technology and cybersecurity] "Beyond NATO’s Madrid Summit: the technological challenge," Real Instituto Elcano, <https://www.realinstitutoelcano.org/en/beyond-nato-madrid-summit-the-technological-challenge/--> AL

First, it will be strategic to make a list of priorities on EDTs in two ways. NATO has already defined seven priority areas, but for each of them it would be advisable to specify their level of criticality. A distinction needs to be made between critical, significant, limited impact and ‘peripheral’ technologies. This is no simple task. It is an effort already developed by some allied countries, such as the recently updated US White House list of critical technologies. The second approach to prioritising some EDTs over others is to make an assessment of the contribution these EDTs make to Alliance defence and security in the short, medium and long terms. Delineating these timeframes can help allocate resources efficiently and avoid potential duplication. This is beneficial both for NATO and for Allies individually, and could prevent the lack of coordination and coherence found in the Inspector General’s 2020 audit on AI projects being developed in the US Department of Defense. Moreover, it is not only beneficial at the tactical level: it can also improve strategic decision-making when it comes to determining what role NATO should play in deterring certain technological developments by third countries. The second challenge is to make innovation projects flexible and agile. The DIANA mechanism will focus on deep technologies, which are the seven priority areas the Alliance has already identified (artificial intelligence, big data processing, quantum technologies, autonomy, biotechnology, novel materials and space), making it necessary for start-ups, research teams and technology companies participating in the network of accelerators and testing centres in more than 20 allied countries to reinvent their projects in the event of failure or non-delivery. Many of the partner countries are also members of the EU. The EU-NATO Joint Declaration is expected to be published later this year to identify lines of cooperation. The NATO Innovation Fund, which is the world’s first multi-sovereign venture capital fund, DIANA, and the EU’s European Innovation Council should work together to enable specialised but small start-ups to grow smoothly. Finally, perception will also be important. Non-NATO countries from the Asia-Pacific area will attend the Madrid Summit, including Australia, Korea, Japan and New Zealand. The first and third cooperate bilaterally with the US through the Quad, Australia already does so through AUKUS and the EU is working on Digital Partnership Agreements with Korea and Japan. Given this multiplicity of initiatives, ensuring mutual trust and confidence in technology projects –within NATO– will be important for their long-term sustainability. Moreover, discussions in recent years about creating a potential NATO policy on China are still incomplete and will be a sensitive issue, as countries have different views on how to engage with China politically, militarily and technologically. In conclusion, the Strategic Concept 2022 is a window of opportunity. And, as such, it will reveal many challenges. Working from the outset with a holistic approach will be a necessary condition for success.

### US Not Key

#### USFG not equipped to handle cyber threats

Jason Smith, 2-22-2022, Jason Smith currently serves as service chair and as assistant professor for security studies at the National War College. He has served as a leader and aviator in the US Coast Guard and the US Army, as advisor to the commandant of the Coast Guard, as senior policy advisor in the US Senate, and on the staff of the National Security Council. "Forget a Whole-of-Government Cybersecurity Strategy—It’s Time for a Whole-of-Nation Approach," Modern War Institute, <https://mwi.usma.edu/forget-a-whole-of-government-cybersecurity-strategy-its-time-for-a-whole-of-nation-approach/> //jsam

Social Contract Theory and Government Response

Increased **familiarity with cyberattacks is accompanied by an understanding of the threat they pose to all aspects of daily life.** It also comes with a growing **frustration of what** many feel is an **ineffective government response to punish those responsible, and to thereby deter others.**

The United States was founded on the ideals of seventeenth-century social contract theory, the intellectual progeny of philosophers like Hobbes, Locke, and Rousseau. They argued that citizens and governments form a contract; the people give up certain freedoms in exchange for government guarantees of law and order. It is this contract that allows for societies to peacefully exist. For example, if Jill is wronged by Jack, Jill does not take the response into her own hands, but trusts the government to represent her interests. The alternative to the social contract is a state of anarchy where might makes right, and thus a failure of civil society.

One of the most understood freedoms given up to the government under social contract theory is security. **The government is responsible for defending society against security threats.** As, the early twentieth-century theorist Max Weber noted, a monopoly on violence is a central attribute of modern states. Concomitantly, it should not be surprising that the US government has vigorously sought to defend its population against physical violence perpetrated both by state actors, as well as by a diverse panoply of violent nonstate actors (e.g., terrorist groups and violent extremists, drug trafficking organizations). However, in broadening the aperture beyond physical security threats to also include those emanating **from the cyber domain, the results become far more mixed.** **While the US government almost certainly desires to be responsive to its citizens cybersecurity needs, it lacks a firm understanding as to how to effectively do so.**

## AT China NB

### Cooperation Good

#### Maintaining balance to US China relations key to mitigate conflict and maintain US heg

Crawford ‘22 (Shannon K. Crawford, 5-26-2022, "Blinken describes delicate balance between isolating and enabling China," ABC News, https://abcnews.go.com/Politics/blinken-describes-delicate-balance-isolating-enabling-china/story?id=84992791)

In the eyes of the Biden administration, **China is a daunting rival and an ever-present risk to global security**. **But** it's **also a necessary partner** for tackling some of the world's most pressing issues. During an address laying out the president's policy towards China, Secretary of State Antony Blinken described a delicate balance between isolating and enabling the country, calling it the "**most serious, long-term challenge" to the global balance**. "**China is the only country with both the intent to reshape the international order and increasingly, the economic diplomatic military and technological power to do it**," he said. "Beijing's vision would move us away from the universal values that have sustained so much of the world's progress over the past 75 years." Blinken boiled the quagmire down into a single phrase. "Put simply, the **United States and China have to deal with each other for the foreseeable future**," he said. "That's why this is one of the **most complex and consequential relationships** of any that we have **in the world** today." The secretary said that while the administration was already employing strategies to curb China's influence, it would not try to limit its growth or create new Cold War. But while Blinken maintained that peace was its core goal, he vowed the U.S. would not compromise it own goals. "**Competition need not lead to conflict. We do not seek it. We will work to avoid it. But we will defend our interests against any threat**," he said. Blinken acknowledged that China had undergone meteoric growth in the past half-century, but said its own people and other countries caught in its crosshairs had paid the price. "Under President Xi, the ruling Chinese Communist Party has become more repressive at home and more aggressive abroad," he said, citing mass surveillance, power grabs in the South China Sea, widespread human rights violations, the subversion of trade rules and more. Blinken also noted the country's repression of freedom in Hong Kong, its brutal treatment of religious and ethnic minorities in Tibet and the Xinjiang region, and its indignation over any international criticism over draconian measures employed against its citizens. "Beijing insists that these are somehow internal matters, that others have no right to raise. That is wrong," Blinken said. The secretary also reaffirmed the One China policy, which was called into question earlier this week when President Biden he would defend Taiwan militarily before walking back his statements. Blinken said the U.S. still acknowledges only one Chinese government, but said its posture towards Taiwan had intensified. "What has changed is Beijing's growing coercion by trying to cut off Taiwan's relations with countries around the world and blocking it from participating in international organizations," he said, adding that China regularly put on shows of force by flying military aircraft near the island. "These words and actions are deeply destabilizing. They risk miscalculation and threaten the peace and stability of the Taiwan Strait." For all its commitment to its own territorial integrity, Blinken argued China's unwavering alliance with Russia was hypocritical. "Even while Russia was clearly mobilizing to invade Ukraine, President Xi and President Putin declared that the friendship between their countries was and I quote, without limits," he said. Blinken repeatedly stressed that the **aim of the administration was not exclude China from the world market**. Instead, senior administration officials say they want to make sure it "plays by the same rules as everyone else." Blinken said that by creating dependencies, Beijing was "seeking to make China less dependent on the world and the world more dependent on China." "For our part, we want trade and investment as long as they're fair, and don't jeopardize our national security," he added. He warned other countries to go into trade partnerships with open eyes, wary of retaliation should they adopt a stance China disagrees with. "Many of our partners already had a painful experience, how Beijing can come down hard when they make choices that it dislikes," he said. The secretary predicted the ideological battle between superpowers would be decided in the next 10 years. "President Biden believes **this decade will be decisive**," Blinken said, outlining the administration's three pronged approach. "The Biden administration strategy can be summed up in three words, invest, align, compete." Invest, he said, referred to invigorating industry, technology and research to ensure the U.S. was up to par with China in these arenas. Align meant strengthening ties with key allies. Blinken said efforts to do both these things were already underway through initiatives like the Bipartisan Infrastructure Law and revived geopolitical partnerships. But to truly compete, he contended that more needed to be done -- calling on Congress to resolve a months' long stalemate and send a massive spending bill aimed at ramping up the country's ability to economically contend with China to the president's desk. "Beijing is determined to lead, but given America's advantages, the **competition is ours to lose** -- not only in terms of developing new technologies, but also in **shaping** how they're used around **the world**, so that they're rooted in democratic values, not authoritarian ones," he implored.

#### China will not upend the liberal world order – It’s not important to compete with China

Williams ’21 (Michael John Williams; senior fellow with the Scowcroft Center’s Transatlantic Security Initiative and associate professor of International Affairs and director of the International Relations Program at the Maxwell School for Citizenship and Public Affairs at Syracuse University; September 21, 2021; Atlantic Council Experts; “Experts react: The AUKUS deal has shaken the transatlantic alliance. What should the US and its allies do now?”; <https://www.atlanticcouncil.org/blogs/new-atlanticist/experts-react-the-aukus-deal-has-shaken-the-transatlantic-alliance-what-should-the-us-and-its-allies-do-now/>; DOA: 7/3/22)

The Biden administration’s refrain of “America is Back” increasingly rings hollow, especially in Europe. While its decision to enter into the AUKUS pact is logical, given its focus on China and the Asia-Pacific region, the way it was reached undermines the very order that the Biden team supposedly wants to uphold. The so-called “liberal world order” (of which the United States is supposedly the guardian) rests upon American hegemony, which itself is premised on the consent of the governed. The foundations of the “liberal world order” are based on the American hegemony in Europe and Asia established after the end of World War II. Although Europe may increasingly seem less important to many officials in Washington, it remains a fundamental base of American legitimacy and power. Yet during a time when Washington seeks to garner allied support to contain China, the Biden administration needs to remember the importance of linkages in foreign policy. France has always been one of the more obstreperous allies, and thus the coarse treatment of Paris with respect to AUKUS will set the stage for increasing discord. AUKUS was a second strike that came on the heels of what Europeans consider to have been a botched withdrawal from Afghanistan—done more via declaration than consultation—which incentivized European allies to view themselves as increasingly distant from the United States. This could have the positive effect of more European capability development, but conversely, it may make European allies less willing to back the United States on other issues. It seems that the Biden administration considers itself the only game in town, and therefore it doesn’t need to worry about what allies think, since there’s no way the European Union could reconcile itself with a Chinese-led world order. This is a dangerous assumption. The American argument is that China will upend the liberal world order. It is true that China does not place much stock in liberal values such as human rights; it is, after all, a market-oriented dictatorship. But this doesn’t mean that China is going to upend the entire international system. Instead, it may seek a global order that is more reminiscent of the past, in which sovereignty and free-market economics reign supreme. This might not be an ideal world from a US point of view—but it may not seem all that bad to the rest of the world.

### Competition Not Key

#### **The US doesn’t need to compete with China.**

Xu and Shen ’19 (Hailin and Yi, head of Fudan University's Cyberspace Governance Research Institute, “With stepped up cyberattacks on China, US seeks online hegemony,” Global Times, June 13, 2019, https://www.globaltimes.cn/content/1153909.shtml)-AT

The US has been accusing China of being the main cybersecurity threat, but based on CNCERT data, US topped the list of sources of such online assaults, Xinhua quoted an expert as saying. In terms of security, the US always adopts double standards. In fact, it has been proved that the US is the principal threat to global cybersecurity. This threat refers not only to Trojan programs that originate in the US; it is probably the only country in the world that pursues offensive cybersecurity strategy and considers a unipolar hegemonic order dominated by it in cyberspace as its strategic goal. What the US is seeking has never been an equal order in cyberspace, but the exclusive freedom of action and asymmetric, US-centered hegemonic order. This is the biggest threat faced by the online world today. We should do away with assumptions that the US is a fair, rational and responsible hegemonic power. It never was, and that is an illusion it has tried to create. In April 2019, the Washington D.C.-based Information Technology and Innovation Foundation found in its research that China "now leads the US" in some scientific and technological areas compared to a decade ago. Although there could be various motives behind the US crackdown on Chinese high-tech enterprises that only the Americans know, we can reasonably conclude that Washington is doing so to seek hegemony in the internet sphere. Washington founded the Cyber Command in 2009 and created 133 Cyber Mission Force teams. Meanwhile in February, US Army General Paul Nakasone, who also directs the National Security Agency, said he wants to recruit more people to these teams. These are some ways the US uses to dominate cybespace, which will definitely add to its military cyber capabilities. On the question of the US girding to launch a cyber war, experts said there is not enough information to support the conjecture. However, what is clear is that there will be no winner in cyber warfare, and China will not be crushed given its might. Washington has listed Beijing as its main target for cyberattacks. Such being the case, what we can do in the first place is to improve our systematic defense capabilities at the national level. President Xi Jinping said in his speech on cybersecurity in April 2016 that the country needs to build and perfect cyber defense and develop its own cyber deterrence capacity. China must augment its cyber defense and deterrence capabilities to prevent rivals from acting - just like the nuclear sphere. Such cyber capability itself is neutral. It can be either defensive or offensive while it can be used to either safeguard peace or dominate the world - depending on which country masters it. As a peace-loving country, China must have sufficient technical capability to maintain peace and defend a just order. The US accuses China and Chinese companies of posing a threat to its national and cybersecurity. In my view, people shouldn't believe a word of Washington's accusations. The US is not a conscientious hegemon but a Janus-faced rogue. Why should we care about what the US says? The halo of a soft power cannot preclude the US from being labeled a cyber hegemon. US President Donald Trump's words and deeds have laid bare Washington's real intentions.

#### American Primacy in Asia is a waste of time and resources

**Roggeveen ’21** (Sam Roggeveen, Director of the Lowy Institute's International Security Program, “The price of American hegemony in Asia,” IPS Journal. 29/9/21. https://www.ips-journal.eu/topics/foreign-and-security-policy/the-price-of-american-hegemony-in-asia-5449/)

Nobody doubts that China is the driving motivation for AUKUS. If China was not undergoing the most rapid maritime modernisation of any country since the US Navy under the Reagan Administration, it is difficult to imagine that Washington would have agreed to sell nuclear technology it has only once before shared with a foreign partner (the UK). Australia has been content to demonstrate its fidelity to its alliance with the US by supporting Washington’s security goals in the Middle East and Afghanistan. Yet that still leaves open a critical question about US grand strategy: are agreements such as AUKUS designed to further America’s ultimate aim of maintaining its status as unrivalled strategic leader of Asia, or is the US willing to share power with China? It is easy to make a case for the first interpretation, at least based on what the United States says. The Trump Administration’s Strategic Framework for the Indo-Pacific, declassified in January 2021, says plainly that the uppermost challenge for US policy in the region is ‘how to maintain US strategic primacy’. President Biden said in March 2021 that ‘China has an overall goal [...] to become [...] the most powerful country in the world [...] That’s not going to happen on my watch’. Yet rhetoric has not been matched by action. America’s military footprint in Asia hasn’t grown much over the last decade, especially when compared to the rapid rise of Chinese military capacity. Obama’s ‘pivot’ to Asia, announced in 2011, is widely acknowledged to have been under-resourced. In that context, AUKUS can be seen a strong sign of American commitment to containing China. Nuclear propulsion technology is closely guarded, so this is much more than an ordinary arms deal; it is a major commitment of American technology. And if primacy is the goal, then Australia has made its clearest commitment yet to supporting it. Australia has been content to demonstrate its fidelity to its alliance with the US by supporting Washington’s security goals in the Middle East and Afghanistan. China clearly means to revise what it regards as a Western imposed rules-based order, and it would probably like to push the US out of the region altogether. It has, however, been less forthright when it comes to issues that directly affect Chinese interests. For instance, despite American encouragement, Australia has still not conducted freedom of navigation missions within 12 nautical miles of China’s artificial islands in the South China Sea. It joined China’s international development bank while Washington remained suspicious. And in 2019 the suggestion that the US might ask Australia to host American intermediate-range missiles on its territory was met with a swift denial by the Morrison Government. That period of reticence appears to be over. As well as the submarine deal, the Australian government is encouraging speculation about permanent American bases in Australia. Is American primacy in Asia worth it? What’s troubling about this is that it implies full confidence in America’s ability to win such a contest for leadership in Asia, and that Australia must do what it can to ensure victory. But China is the biggest challenger the US has ever faced. As former Brookings scholar and now China adviser in the National Security Council Rush Doshi has observed, in the last century no American adversary or coalition of adversaries has ever reached 60 percent of US GDP. China passed that mark as early as 2014. It’s an arresting statistic, which should encourage Australian policy-makers to ask if the maintenance of American primacy in Asia is a realistic or even worthwhile goal. US primacy has certainly been advantageous for Australia, but the price of keeping America at the top is now rising dramatically. European powers should also be asking themselves about their interests in Asia. Australia’s decision to commit to either American or British nuclear-powered submarines meant that the deal to buy French boats had to be cancelled, leading to much introspection about France’s future role in the Pacific. Britain’s involvement in AUKUS has also raised questions about its ambitions in this part of the world. In June, NATO identified China as a ‘systemic challenger’. But it is difficult to see what vital strategic interest is at stake for NATO and the European powers in Asia. China clearly means to revise what it regards as a Western imposed rules-based order, and it would probably like to push the US out of the region altogether. However, that is not enough reason for Europe to involve itself in a power struggle against a nation that offers massive economic opportunity, but which poses no military threat to Europe.

### Not Zero Sum

#### Focus is not zero sum – US can defend against China and Russia

Kroenig 22 [Kroenig, Matthew. Matthew Kroenig is deputy director of the Atlantic Council’s Scowcroft Center for Strategy and Security and a professor in the Department of Government and the Edmund A. Walsh School of Foreign Service at Georgetown University. His latest book is The Return of Great Power Rivalry: Democracy Versus Autocracy From the Ancient World to the U.S. and China. "Washington Must Prepare For War With Both Russia And China". Foreign Policy, 2022, https://foreignpolicy.com/2022/02/18/us-russia-china-war-nato-quadrilateral-security-dialogue/. Accessed 3 July 2022.]//DL

As Russia threatens the largest land invasion in Europe since World War II, the most consequential strategic question of the 21st century is becoming clear: How can the United States manage two revisionist, autocratic, nuclear-armed great powers (Russia and China) simultaneously? The answer, according to many politicians and defense experts, is that Washington must moderate its response to Russia in Europe to focus on the greater threat posed by China in the Indo-Pacific. This would be a mistake. **The United States** remains the world’s leading power with global interests, and it **cannot afford to choose between Europe and the Indo-Pacific.** Instead, Washington and its allies should develop a defense strategy capable of deterring and, if necessary, defeating Russia and China at the same time. In recent weeks, Biden has sent several thousand U.S. troops to reinforce NATO’s eastern flank—and for good reason. A major war in Ukraine could spill across international boundaries and threaten the seven NATO allies that border Russia, Belarus, and Ukraine. Moreover, if Russian President Vladimir Putin succeeds in Ukraine, why would he stop there? Putin has shown a clear interest in resurrecting the former Russian Empire, and other vulnerable Eastern European countries—Poland, Romania, or the Baltic states—might be next. A successful Russian incursion into a NATO ally’s territory could mean the end of the Western alliance and the credibility of U.S. security commitments globally. The threat posed by China is also serious. Adm. Philip Davidson, former commander of U.S. Indo-Pacific Command, predicted China could invade Taiwan within the next six years. This is a war the United States might lose. If China succeeds in taking Taiwan, it would be well on its way to disrupting the U.S.-led order in Asia, with an eye to doing the same globally. Moreover, Russia and China are increasingly working together. As this month’s summit between Putin and Chinese President Xi Jinping shows, Moscow and Beijing are forging a closer strategic partnership, including on military matters. These dictators could coordinate dual attacks on the U.S. alliance structure or opportunistically seize on the distraction provided by the other’s aggression. In other words, there is a serious risk of simultaneous major-power wars in both Europe and the Indo-Pacific. To address this problem, many have proposed answers that simply will not work. The Biden administration initially hoped to put relations with Russia on a “stable and predictable” footing to focus on China, but Putin had other ideas, as the world is now seeing in Ukraine. Unfortunately, Washington does not get to decide how its adversaries sequence their aggression. Others have expressed hope that Washington can peel these powers apart or even align with Russia against China, but these are not realistic solutions. The misguided view gaining the most recent acceptance, however, is that Washington should simply choose the Indo-Pacific over Europe. Politicians and experts argue that the United States lacks the resources to take on both Russia and China. They point to China’s power and Asia’s wealth and argue that Asia should be the priority. While Washington pivots to Asia, wealthy European countries, such as Germany, should step up to provide for NATO’s defense. Indeed, the Biden administration’s National Defense Strategy, which has been delayed due to the Ukraine crisis, is expected to focus on China without offering a clear solution to the two-front-war problem. A good strategy, however, starts with clear goals, and Washington’s objectives are to maintain peace and stability in both Europe and Asia. U.S. interests in Europe are too significant to let them be worked out solely between Putin and the United States’ European allies. Indeed, the European Union, not Asia, is the United States’ largest trade and investment partner, and this imbalance is much starker when China (which the United States seeks greater economic decoupling from), is removed from the equation. Furthermore, China has conducted military exercises in Europe and the Middle East. Competing with China militarily means competing globally, not just in Asia. In addition, Xi is gauging U.S. resolve, and a weak response in Ukraine might make a Chinese move on Taiwan more likely. Moreover, the United States is not France; it is not compelled to make gut-wrenching strategic choices about its national security due to constrained resources. In short, publishing a defense strategy that can only handle one of the United States’ great-power rivals (which is what is expected from the forthcoming national defense strategy) is planning to fail. Instead, the United States and its allies must design a defense strategy capable of deterring and, if necessary, defeating both Russia and China in overlapping time frames. The pause in releasing Biden’s defense strategy provides an opportunity to go back to the drawing board and get this right. To be sure, developing such a strategy will be challenging, but there are a number of ways to begin to square the circle. First, Washington should increase defense spending. Contrary to those who claim that constrained resources will force tough choices, the United States can afford to outspend Russia and China at the same time. The United States possesses 24 percent of global GDP compared to a combined 19 percent in China and Russia. This year, the United States will spend $778 billion on defense compared to only $310 billion in Russia and China. Moreover, the United States could go so far as to double defense spending (currently 2.8 percent of GDP) and still remain below its Cold War average (close to 7 percent of GDP). Indeed, given that this new Cold War is every bit as dangerous as the last one, a meaningful increase in defense spending, focused on the 21st century’s emerging defense technologies, is in order. Some might argue that the days of a U.S. economic advantage are numbered due to China’s rise, but China’s internal dysfunctions are catching up with it. Dictators like Xi prioritize political control over economic performance. Xi is undermining China’s growth model by cracking down on the private sector and rolling back liberalizing reforms, and his aggressive diplomacy is upsetting international economic relationships. As a result, Beijing’s economy is stagnating. Russia’s long-term economic outlook is even worse. In short, even if this new strategic competition becomes a two-versus-one arms race, Washington is likely to prevail. In addition, the United States can actively lead its allies in Europe and the Indo-Pacific to develop a free world defense strategy. The United States and its formal treaty allies possess nearly 60 percent of global GDP, and together, they can easily marshal the resources to maintain a favorable balance of military power over both China and Russia. Preexisting formal alliances like NATO in Europe and bilateral alliances in Asia can be supplemented with new arrangements, such as the Quadrilateral Security Dialogue. European allies should invest in armor and artillery while Asian allies buy naval mines, harpoon missiles, and submarines. Allies do need, therefore, to step up and do more for their defense, but they will not do it on their own if the United States threatens to leave Europe. Instead, Washington should actively lead, moving from a model where Washington provides defense to allies to one where Washington contributes to allies’ self-defense. This should include incorporating key allies into military planning, sharing responsibilities, and devising a rational division of labor for weapons acquisition. European allies should invest in armor and artillery while Asian allies buy naval mines, harpoon missiles, and submarines. The U.S. Army should prioritize Europe while the U.S. Navy takes the Indo-Pacific and a larger U.S. Air Force plays a significant role in both theaters. In addition, the United States should provide strategic capabilities like its nuclear umbrella; global conventional strike capabilities, including hypersonic missiles; and intelligence, surveillance, and reconnaissance. Finally, if necessary, Washington could always take a page from its Cold War playbook and rely more heavily on nuclear weapons to offset the local, conventional advantages of its rivals. The presence of U.S. tactical nuclear weapons in Europe helped deter the massive Soviet Red Army for decades. Similarly, the United States could rely on threatening nonstrategic nuclear strikes to deter and, as a last resort, thwart a Chinese amphibious invasion of Taiwan or a Russian tank incursion into Europe. To be sure, there are risks associated with nuclear deterrence, but nuclear weapons have played a foundational role in U.S. defense strategy for three-quarters of a century—and will likely continue to do so for decades to come. **Deterring China and Russia at the same time will not be easy, but it is better than pretending Washington can deal with one major-power rival or the other at its convenience**. Thank goodness, former U.S. President Franklin Roosevelt did not choose victory in only one theater during World War II. **Biden should** follow his exampl**e and plan to defend U.S. interests in Europe and the Indo-Pacific at the same time.**