# 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.**