# CIVIL-MILITARY COUNTERPLAN

## NEG

### #

#### The United States federal government should increase civil-military cooperation with the North Atlantic Treaty Organization in the area of \_\_\_\_.

#### Public-private partnerships are key to emerging tech integration.

Nadja El Fertasi 06-22-2019 [El Fertasi has built a career path in NATO over the past seventeen years taking on a variety of posts in different fields within large multinational NATO institutions. She holds a Master’s degree in International relations from the University of Cambridge and is an alumna of the NATO-wide Executive Development Program, Information and Security, “Why Digital Ecosystems of Civil-Military Partnerships Are a Game Changer for International Security and Defence,” https://procon.bg/system/files/4202\_elfertasi\_digital\_ecosystems.pdf//ZW]

Institutional Challenges Facing NATO NATO as an institution continues to face a myriad of challenges trying to adapt to a digital era. NCI Agency’s General Manager vision “NATO’s Digital Endeavour” goes a long way in articulating these challenges and implementing solutions through a phased approach and help bring NATO amongst the digital natives.16 Some core issues are still likely to hamper any progress if not addressed. First, if we look at a multinational security institution consisting of 29 member nations which have different interests and pace of technological innovation, the gap between the USA and its Allies in Europe is still prevalent.17 Change and progress will happen but is likely to be slower as large and traditional multinational security institutions are not driven by the same business models as corporate organizations in the private sector. Furthermore, digital transformation should be seen as a journey rather than an end state for it to be successfully implemented. Second, adopting an end-to-end approach in any digital endeavour requires partnerships and agreements between public and private sectors as ownership of digital assets are fragmented across the civil-military spectrum. Finally, the private sector, especially small and medium-sized enterprises and start-ups have a lot to offer in developing niche, cutting-edge, disruptive technology. Working with next-generation technology can bring information superiority for the defence sector to another level. Still, large institutions like NATO remain a black box for these industries to work with.

#### Effective P3’s are key to outpace adversary innovation

Justin Magula and Paula Alvarez-Couceiro 09-30-2019 [Justin Magula is an Army Strategist with four combat deployments, serving in the Strategic Landpower and Futures Group at the U.S. Army War College, Paula Alvarez-Couceiro is a recent graduate of Strategic Studies at the Johns Hopkins University School of Advanced International Studies, Wavell Room, “Maintaining and Improving NATO’s Technical Edge,” https://wavellroom.com/2021/09/30/maintaining-improving-natos-technological-edge-technology///ZW]

What happens when an alliance’s competitors quickly improve their technology and capabilities to place the alliance at increased risk? The North Atlantic Treaty Organization (NATO) addressed this dilemma during a recent summit in Brussels. At the summit, the North Atlantic Council built upon NATO’s 2030 strategic outline and presented targets for increased technological collaboration to counter growing threats from Russia, China, and non-state actors. While NATO’s scientific and technical superiority has historically allowed it to outpace competitors, its adversaries are quickly closing the gap. NATO members still hold advantages in their development of new technologies. According to the Global Innovation Index, seven of the top ten most innovative countries globally are part of NATO, while the other three are key NATO partners. Even so, NATO can do more to harness the alliance’s combined technological prowess to better compete and win in a future conflict. As China seeks to become the world’s innovation leader and Russia continues to undermine the alliance’s security, NATO will need to out-innovate its competitors and prepare for an uncertain future. Four areas where NATO can focus on improving its competitive edge are developing its formal organizations, increasing public and private sector collaboration, harnessing and countering Emerging Disruptive Technologies (EDTs), and improving conventional military equipment. NATO must maintain its relative lead in technology sectors to defend its people and enhance its long-term strategic position. Improving science and technology (S&T) innovation will increase alliance collaboration, strengthen public and private sector cooperation, counter hybrid threats, deter adversaries, and harden defenses against attacks. NATO’s effectiveness in the future will heavily depend on its ability to maintain and improve its science and technology capabilities. A Changing Environment The global geopolitical situation has changed significantly over the past decade. Although NATO remains the world’s most successful and powerful alliance, China and other adversaries are quickly reducing NATO’s military and scientific advantages. In just the past year, China raised its defense budget by 6.8 percent and continues to build global power projection capabilities in addition to its regional defenses. As part of what some call a Fourth Industrial Revolution,Beijing is rapidly investing in AI, biotechnology, robotics, and other new technologies. Russia is also developing new technologies, especially in areas where it can exploit NATO’s weaknesses. Russia’s ballistic missiles can reach anywhere in Europe, and Russia has placed renewed emphasis on improved missile technology, such as recent hypersonic advances. Russia has built a robust Anti-Access Area Denial (A2AD) network on Europe’s eastern flank while simultaneously expanding military capabilities into its Arctic region. Both areas pose direct security challenges to NATO, which the alliance’s S&T efforts can help mitigate. Over the past decade, NATO has recognized the need for increased innovation and technological advancements. In 2012, the alliance created the Science and Technology Organization, taking on the former roles of the NATO Research and Technology Organization, including its executive function. It also incorporated the former NATO Undersea Research Center, established the NATO Chief Scientist position, and outlined the unified governance of NATO S&T. In 2020, NATO created an Innovation Board and an Advisory Group on Emerging and Disruptive Technologies to provide external advice to NATO on optimizing its innovation efforts. At the 2021 Brussels Summit, NATO agreed to launch a civil-military Defense Innovation Accelerator for the North Atlantic (DIANA) to “foster transatlantic cooperation on critical technologies, promote interoperability and harness civilian innovation by engaging with academia and the private sector, including start-ups.” There are plans to establish a NATO Innovation Fund (NIF), where allies “can support start-ups working on dual-use emerging and disruptive technologies in areas key to Allied security.” These are steps in the right direction, but NATO can do more. Expanding Technological Organizations In conjunction with its newest additions, the DIANA and NIF, NATO can expand the capacities of its Science and Technology Organization (STO) to boost research and development (R&D) in artificial intelligence (AI), missile and missile defense technology, space, cyber, and other EDTs. The STO is the world’s largest defense and security research forum, employing over 6,000 scientists from allied nations. However, the STO does not turn NATO defense spending into tangible products or equipment for the alliance. NATO could use the STO to streamline research and product development, ensuring all allies are working toward a common goal and not spending resources on identical R&D. For instance, each country could allocate part of its defense budget to develop standardized systems like integrated air, missile, and cyber defenses. Whether using the STO or DIANA as its main innovation driver, NATO must continue developing its formal institutions to harness solutions that benefit the entire alliance and help it achieve its three core tasks of collective defense, crisis management, and cooperative security. Public and Private Sector Collaboration The Brussels Summit Communique also recommends continuing the R&D of AI technologies and identifying alliance gaps in this critical focus area. Many of these advancements occur in the private sector, and NATO must find ways to use those technologies for the alliance. The U.S. National Security Commission on Artificial Intelligence’s March 2021 report states that AI-enabled warfare is part of the near future. While the United States and NATO are currently ahead in these technologies, other countries will soon pass them unless they increase their R&D efforts. In addition to boosting research through the STO and DIANA, NATO can streamline the acquisition of commercial sector AI-focused technologies for national security purposes and create an alliance-wide process that acquires emerging technologies from the private sector. The rapidly changing nature of emerging technologies and the quantity and depth of innovation seen in the private sector require an acquisitions system that is not only fast but allows for the rapid integration of updated product iterations and innovations. Autocratic competitors excel in private and public sector integration, given the nature of their systems. Improving its ability to apply privately developed technology for military uses rapidly will ensure that NATO retains its competitive edge over its predominantly autocratic adversaries. Harnessing and Countering Emerging Disruptive Technologies While emerging and disruptive technologies (EDTs) touch all aspects of life and present exciting opportunities for the alliance, they also present threats. Many of NATO’s adversaries use EDTs against alliance personnel and infrastructure, such as recent cyberattacks targeting Polish politicians and the Colonial Pipeline. Enhancing its innovation processes will allow NATO to improve its military technology across all domains and boost its deterrence and defense capabilities. NATO could then better deter Russian and Chinese hybrid threats in cyber, space, electronic warfare, and information domains. For instance, NATO can use its forthcoming Cyber Command to take collective action and demonstrate cyberspace thresholds that will result in unified offensive cyber or conventional responses if crossed by its adversaries. By strengthening its cyber abilities and adding new capabilities, NATO can deter adversaries in the information space and take the offensive against them. NATO would then rob Russia and China of success in areas where they currently excel, and better protect the alliance’s people and infrastructure. Conventional Military Improvements NATO can also use its technological advancements to improve its conventional military capabilities. One critical area where NATO must focus is its integrated air and missile defense. Russian nuclear weapons can reach anywhere in Europe and NATO cannot adequately defend against new technologies like swarm warfare or hypersonic missiles. Two of NATO’s high-visibility modernization programs focus on combating air and missile threats, but NATO must do more to combat emerging and future adversary weapons. As the United States continues R&D on a Patriot missile system replacement, NATO countries could ingrate into its supply chain, like that of the F-35 aircraft, or develop complementary systems that fill gaps in the U.S. air defense system’s effectiveness. The current NATO Integrated Air and Missile Defense system uses mainly American-made radars and missiles stationed in NATO countries. While effective, NATO could harden its defenses by fielding European-developed systems that are compatible with current and future U.S. systems, thus expanding its anti-access area denial (A2/AD) bubble while simultaneously reducing air and missile threats. Furthermore, the alliance can conduct more combined military exercises to test new equipment and boost unit proficiency. Improving its deterrence and defenses in critical areas will reduce the military threats from NATO’s adversaries as they seek to sow division and destabilize the alliance. When it couples military advances with other areas of technological improvement, NATO gains the best chance of maintaining its competitive edge. NATO will still need to overcome bureaucratic hurdles across its 30-member alliance. As Nicholas Nelson of the Center for European Policy Analysis (CEPA) notes, for the DIANA and NIF “to succeed, they must address authority and budget concerns, and then bring in the right personnel to lead and staff them.” Even so, NATO is taking the proper steps to improve its scientific and technological capabilities. Its strategic documents reflect the importance it is placing in these areas. By creating new institutions, NATO is setting the foundation for further development and expanded capabilities. Given the threats that adversaries pose to the alliance, maintaining and improving its scientific and technological prowess will be vital to NATO’s future success. Strengthening these areas will boost military effectiveness, deterrence, and defense and enhance private and public cooperative advancements. It will ultimately give the alliance more strategic flexibility while improving NATO’s defenses in areas beyond the military, such as energy and cybersecurity in the private sector. By continuing to out-innovate its competitors, NATO will protect its people and infrastructure, and ensure that the alliance remains prepared to combat any challenges from Russia or China.

#### Adversary innovation-lead causes nuclear war

Kroenig & Gopalaswamy 18, \*Associate Professor of Government and Foreign Service at Georgetown University and Deputy Director for Strategy in the Scowcroft Center for Strategy and Security at the Atlantic Council \*\*Associate Professor of Government and Foreign Service at Georgetown University and Deputy Director for Strategy in the Scowcroft Center for Strategy and Security at the Atlantic Council (\*Matthew Kroenig \*\*Bharath Gopalaswamy, 11-12-2018, "Will disruptive technology cause nuclear war?," Bulletin of the Atomic Scientists, <https://thebulletin.org/2018/11/will-disruptive-technology-cause-nuclear-war/>)

Recently, analysts have argued that emerging technologies with military applications may undermine nuclear stability (see here, here, and here), but the logic of these arguments is debatable and overlooks a more straightforward reason why new technology might cause nuclear conflict: by upending the existing balance of power among nuclear-armed states. This latter concern is more probable and dangerous and demands an immediate policy response. For more than 70 years, the world has avoided major power conflict, and many attribute this era of peace to nuclear weapons. In situations of mutually assured destruction (MAD), neither side has an incentive to start a conflict because doing so will only result in its own annihilation. The key to this model of deterrence is the maintenance of secure second-strike capabilities—the ability to absorb an enemy nuclear attack and respond with a devastating counterattack. Recently analysts have begun to worry, however, that new strategic military technologies may make it possible for a state to conduct a successful first strike on an enemy. For example, Chinese colleagues have complained to me in Track II dialogues that the United States may decide to launch a sophisticated cyberattack against Chinese nuclear command and control, essentially turning off China’s nuclear forces. Then, Washington will follow up with a massive strike with conventional cruise and hypersonic missiles to destroy China’s nuclear weapons. Finally, if any Chinese forces happen to survive, the United States can simply mop up China’s ragged retaliatory strike with advanced missile defenses. China will be disarmed and US nuclear weapons will still be sitting on the shelf, untouched. If the United States, or any other state acquires such a first-strike capability, then the logic of MAD would be undermined. Washington may be tempted to launch a nuclear first strike. Or China may choose instead to use its nuclear weapons early in a conflict before they can be wiped out—the so-called “use ‘em or lose ‘em” problem. According to this logic, therefore, the appropriate policy response would be to ban outright or control any new weapon systems that might threaten second-strike capabilities. This way of thinking about new technology and stability, however, is open to question. Would any US president truly decide to launch a massive, bolt-out-of-the-blue nuclear attack because he or she thought s/he could get away with it? And why does it make sense for the country in the inferior position, in this case China, to intentionally start a nuclear war that it will almost certainly lose? More important, this conceptualization of how new technology affects stability is too narrow, focused exclusively on how new military technologies might be used against nuclear forces directly. Rather, we should think more broadly about how new technology might affect global politics, and, for this, it is helpful to turn to scholarly international relations theory. The dominant theory of the causes of war in the academy is the “bargaining model of war.” This theory identifies rapid shifts in the balance of power as a primary cause of conflict. International politics often presents states with conflicts that they can settle through peaceful bargaining, but when bargaining breaks down, war results. Shifts in the balance of power are problematic because they undermine effective bargaining. After all, why agree to a deal today if your bargaining position will be stronger tomorrow? And, a clear understanding of the military balance of power can contribute to peace. (Why start a war you are likely to lose?) But shifts in the balance of power muddy understandings of which states have the advantage. You may see where this is going. New technologies threaten to create potentially destabilizing shifts in the balance of power. For decades, stability in Europe and Asia has been supported by US military power. In recent years, however, the balance of power in Asia has begun to shift, as China has increased its military capabilities. Already, Beijing has become more assertive in the region, claiming contested territory in the South China Sea. And the results of Russia’s military modernization have been on full display in its ongoing intervention in Ukraine. Moreover, China may have the lead over the United States in emerging technologies that could be decisive for the future of military acquisitions and warfare, including 3D printing, hypersonic missiles, quantum computing, 5G wireless connectivity, and artificial intelligence (AI). And Russian President Vladimir Putin is building new unmanned vehicles while ominously declaring, “Whoever leads in AI will rule the world.” If China or Russia are able to incorporate new technologies into their militaries before the United States, then this could lead to the kind of rapid shift in the balance of power that often causes war. If Beijing believes emerging technologies provide it with a newfound, local military advantage over the United States, for example, it may be more willing than previously to initiate conflict over Taiwan. And if Putin thinks new tech has strengthened his hand, he may be more tempted to launch a Ukraine-style invasion of a NATO member. Either scenario could bring these nuclear powers into direct conflict with the United States, and once nuclear armed states are at war, there is an inherent risk of nuclear conflict through limited nuclear war strategies, nuclear brinkmanship, or simple accident or inadvertent escalation. This framing of the problem leads to a different set of policy implications. The concern is not simply technologies that threaten to undermine nuclear second-strike capabilities directly, but, rather, any technologies that can result in a meaningful shift in the broader balance of power. And the solution is not to preserve second-strike capabilities, but to preserve prevailing power balances more broadly. When it comes to new technology, this means that the United States should seek to maintain an innovation edge. Washington should also work with other states, including its nuclear-armed rivals, to develop a new set of arms control and nonproliferation agreements and export controls to deny these newer and potentially destabilizing technologies to potentially hostile states. These are no easy tasks, but the consequences of Washington losing the race for technological superiority to its autocratic challengers just might mean nuclear Armageddon.

### Solvency

#### Public-private partnership solves.

James Stavridis and Evelyn N. Farkas 03-19-2012 [Admiral James Stavridis is the Supreme Allied Commander Europe (SACEUR) and Commander, U.S. European Command (EUCOM), Evelyn N. Farkas is his Senior Advisor for Public–Private Partnership. Any reference to non-Federal entities in this article should not be construed as an endorsement by the U.S. Department of Defense of these entities, their products, or services, The Washington Quarterly Volume 35, Issue 2, “The 21st Century Force Multiplier: Public-Private Collaboration,” https://doi.org/10.1080/0163660X.2012.665336//ZW]

The Case for Collaboration: Effectiveness and Efficiency Public–private collaboration generally falls into several broad categories of activities: 1) sharing expertise; 2) exchanging information; and 3) executing projects and operations. Both parties benefit in tangible and intangible ways. For the government, the key advantage is access to expertise, analysis, skills, perspective, and resources not always available in the public sector. In the current fiscally-constrained environment, the benefits of such collaboration to the government are obvious. Efficiency—saving money and other resources—accrues, and with the added private sector skills, insights, and resulting innovation, so does effectiveness. Like their business counterparts, these public-sector practitioners manage people, finances, organizational change, and “back office” operations every day. Sharing best practices—or in some cases, the worst ones—can be educational for those who manage our national security entities. The private sector also offers an agility not often found in government. One NGO representative working to help veterans explains, “If NGO programs prove less effective or [the] needs shift, NGO programs are easier to end than a government program.”7 As President Ronald Reagan quipped, “A government bureau is the nearest thing to eternal life we'll ever see on this Earth.”8 Businesses can often “fail” faster than their public counterparts, adopting lessons learned and forging ahead. It used to be that the government drove innovation across all sectors; that is no longer true. It used to be that the government drove innovation across all sectors in its defense and science laboratories, reducing the incentive for collaboration. That is no longer true. Much of the cutting edge work is now being done in the private sector. This is most obvious today in the field of computer and information technology, but extends to energy and nanotechnology, among other areas. As a result, the government relies on private sector expertise to maintain its lead in defense, space, and other endeavors related to national security. This dependency means that the government is also affected by private sector vulnerabilities—probably even beyond areas where the private sector has the technological lead. Through collaboration regarding, for example, shared threats on financial fraud and economic espionage, both government and industry can keep abreast of developing challenges. The QDDR speaks for the State Department, USAID, and beyond when it asserts, “Private sector partners can add value to our missions through their resources, their capacity to establish presence in places we cannot, through the technologies, networks and contacts they can tap, and through their specialized expertise or knowledge.”9 For corporate or non-profit entities, collaboration with the government may offer access to information and sometimes intelligence, as well as legitimacy. The private sector often lacks the necessary information and/or ability to coordinate entities that often value their privacy and autonomy over concerted effective action. This is why protection of critical infrastructure—both brick-and-mortar and virtual—is a public–private effort. The government can serve as the honest broker to which corporations may safely disclose vulnerabilities or proprietary information, which the government can use to devise appropriate means to protect all corporations and society. Other issues, such as caring for wounded veterans, are best addressed through a comprehensive approach—which entails responsibilities for the government to provide health care and other support as well as for private organizations and individuals to provide employment and social support. And operating overseas, the government often has long-term international networks via its embassies, which even older corporations cannot replicate. Finally, of course, governments can offer access to funding. In order to tap into the best minds and technology, the government must pay for it, or appeal to American philanthropy and patriotism. The appeal and response bring another benefit to government and society: promoting social service and responsibility. Organizations that team up with the government—especially when there is no direct business or personal gain involved—can foster patriotism, civic participation, and even raise public support for government and good governance. Individuals who engage with government in this manner gain a sense of accomplishment, lending their knowledge to our foreign-policy and national-security goals. Businesses can also bolster their public image through collaboration billed as “pro bono,” or “corporate social responsibility.” Neville Isdell, the former Chairman and CEO of The Coca Cola Company, advocates “connected capitalism,” a system whereby businesses connect with governments, non-profits, and civic society to shape their core business strategies in ways that foster sustainable and profitable commercial growth *and* contribute to addressing social problems. He works to recruit corporations that pledge to partner with governments, communities, and NGOs to simultaneously further corporate interests and improve society. His motivation, in part, is a desire to help capitalism—which he perceives as currently under attack worldwide—evolve in order to survive.10 Executives from General Electric, Sun Trust Bank, and United Parcel Service have signed up to Isdell's effort and their partners include CARE and USAID. Non-profit research institutes, universities, advocacy organizations, and humanitarian organizations can also benefit from an association with the government by burnishing their credentials as purveyors of knowledge and expertise, or as agile, relevant actors. To the extent that the public views the government or its representatives, such as military officers, favorably and trusts it to seek qualified collaborators who have skill and integrity, private entities and individuals can elevate their public image. Despite this, sometimes private entities and individuals prefer to work in collaboration with the government as separate entities, as opposed to joining the government as employees or contractors. This is true for Blue Star Families (BSF), a non-profit supporting and advocating for military families. “Public–private partnerships are key to BSF's philosophy. Military families serve and sacrifice because we parents, spouses, and children love our service member, and love our country, not because we love the Pentagon. In fact, many families prefer not to interact with ‘official channels.’ So it is right and fitting that the responsibility for helping families falls not only to the Pentagon or the individual services, but to the larger society as well.”11

#### NATO P3 coop solves democracy and disinformation.

Brittany Beaulieu and David Salvo 07-2018 [David Salvo is deputy director of the Alliance for Securing Democracy at The German Marshall Fund of the United States, Brittany Beaulieu is a fellow and program officer at the Alliance for Securing Democracy at The German Marshall Fund of the United States, Alliance for Securing Democracy, “NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence,” https://www.jstor.org/stable/pdf/resrep18856.pdf//ZW]

NATO should further develop public-private partnerships with civil society. NATO should increase its efforts to develop partnerships with local civil society organizations that can combat disinformation, play the role of the “watch dog” in holding political elites to standards of transparency, and advocate for democratic ideals and principles at the grassroots level. It should also devote additional resources to public diplomacy campaigns, such as the #WeAreNATO campaign, and engage all member states in their coordination. New campaigns could target citizens in rural areas who do not use Facebook or Twitter by engaging them at schools, libraries, and community and retirement centers.

#### PPP is the answer to cyber governance.

Kristoffer Kjærgaard Christensen and Karen Lund Petersen 11-2017 [Kristoffer Kjærgaard Christensen is PhD from the University of Copenhagen, Department of Political Science. His research is on the significance of cyber security for contemporary security politics, looking at how cyber security involves new security actors and contributes to creating new political spaces and understandings of (security) politics and democracy, Karen Lund Peteresen is a PhD from the University of Copenhagen. Her research focuses on the transnationalisation of private sector responsibilities on security; political risk; intelligence; and new forms of strategic thinking in the management of international threats, International Affairs Volume 93 Issue 6, pgs. 1435-1452, “Public-private partnerships on cyber security: a practice of loyalty,” https://doi.org/10.1093/ia/iix189//ZW]

Owing to the complex, dynamic and dispersed nature of information and communication technology (ICT), cyber-security risks are not easily managed. ICT is everywhere. It not only transcends national jurisdictions but has found its way into nearly all spheres of modern life. Critical infrastructure, private businesses and the most intimate aspects of our daily lives are all affected by ICT, not least through the expanding internet of things.5 This development drastically increases the potential vectors of vulnerability and expands their scope to a plethora of different actors—from states to private companies and individual users. Moreover, the networked nature of ICT means that cyber-security risks are not limited to a particular physical location. Cyber attacks may potentially come from anywhere. In short, cyber security is characterized by a fundamental uncertainty. This uncertainty and the diversity of actors affected pose a great challenge to the governance of cyber-security risks and call for new modes of organizing security practices. In this regard public–private partnerships (PPPs) are often seen as ‘the answer’ to many of the challenges related to cyber-security governance: PPPs are, in policy as well as academic circles, often considered a mode of organization that can enhance flexibility and robustness by including a broader range of civil and private actors. In partnership meetings private businesses are called upon to voluntarily share knowledge on national security and to assume responsibility for ensuring an effective management of cyber threats.6 Despite a strong agreement about the characterization of cyber-security risk as a ‘shared risk’, the turn to partnerships does not itself establish what kind of knowledge the different partners should share with each other. Rather, the fundamental uncertainty associated with cyber security seems to have opened up the space for contestation over ‘what to counter’, and thus what counts as cyber-security knowledge.

### Solvency---Companies Say Yes

#### Companies say yes

Marian L. Lawson 10-28-13 [Specialist in Foreign Assistance Policy, Congressional Research Service, “Foreign Assistance: Public-Private Partnerships (PPPs),” https://sgp.fas.org/crs/misc/R41880.pdf//ZW]

Potential Benefits of Public-Private Partnerships PPPs have become more common because both public and private partners believe PPPs achieve shared goals more effectively than each partner could by acting alone. Commonly cited advantages of PPPs include the following: • Shared Risks and Resources. While development officials are quick to point out that PPPs are not primarily a means of saving taxpayer dollars, sharing the cost and financial risks of development activities is a key attraction of modern partnerships that involve joint resource contributions. Both the government and private entities are sometimes willing to participate as partners in a project they would not be able or willing to support in its entirety. Partnership may also allow for project implementation on a larger scale, and for cost savings based on scale, resulting in each partner achieving a greater development return on its investment (or a diluted cost of failure). • Sustainability. A common criticism of traditional development activities is that they never become self-sustaining and fade away when government funding ends. PPPs attempt to avoid this problem by tapping into core business interests and making sustainability profitable. In the SUCCESS Alliance, for example, small Vietnamese cocoa farmers were integrated into Mars’s global supply chain, having elevated their cocoa production and processing to international standards with assistance from USAID, Mars, and the World Cocoa Foundation. In theory, market demand should sustain the partnership and the improved farmer incomes. While the sustainability argument seems logical and is supported by anecdotal evidence, there has been no comprehensive study of how PPP sustainability compares to that of non-PPP approaches. • Market Access/Networks. Corporations and private entities often have networks of customers, suppliers, supporters, and employees that can broaden the reach of a development program beyond where a development agency could go. By partnering with MTV in several regional alliances, for example, USAID tapped into a vast global audience of young people for its messages against human trafficking and promoting HIV/AIDS prevention in the EXIT alliance. MTV, for its part, saw an opportunity for positive public relations and an association with USAID that could potentially enhance its reputation in developing countries. • Technology and Intellectual Property. Effective use of technology, which many experts believe is crucial to economic development, can be a daunting challenge in developing countries. Through partnering with Cisco, Microsoft, and other global technology companies, development agencies are able to overcome technical, legal, and financial barriers to accessing certain technology. The technology companies, in turn, are developing relationships and support infrastructure to position themselves to compete for the next generation of technology consumers, many of whom will live in developing countries. • Cutting-Edge Business Practices. While USAID and other federal aid agencies can provide technical expertise in a wide range of development sectors, they often do not have the specialized industry knowledge that a private company has. In Guatemala’s Inclusive Market Alliance for Rural Entrepreneurs (IMARE), for example, Walmart supplies crucial market information that augments the impact of technical assistance and access to credit provided through NGO partners by enabling better farm planning and quality control of targeted crops. More than 600 rural small-scale farmers earned higher incomes by selling to the region’s largest retailer, while Walmart strengthened its supply chain.39 In partnering with Sesame Street, USAID gained access to advanced pedagogy and production capacity, while Sesame Street was able to extend its global reach into more developing countries. Reputation Enhancement. Positive public relations are often a significant consideration for corporate entities entering into PPPs. Partnering with a U.S. government entity can lend legitimacy to a private entity, and association with development activities can enhance a corporation’s reputation for being socially responsible. The Small Export Vegetable Alliance in Zambia, for example, was inspired in part by private sector partner Agroflora’s desire to project a more populist image. The company was concerned that land seizures in neighboring Zimbabwe could spread to Zambia and affect its business if it was not seen as benefitting smallholder Zambian farmers.40 Participating organizations and corporations may also anticipate that partnerships will improve their relationships with national and community leaders.

### Solvency---Space

#### P3s solve space--- incentivize innovation and datasharing.

Karen Jones 04-2018 [Karen L. Jones is a senior project leader with The Aerospace Corporation’s Center for Space Policy and Strategy, The Aerospace Corporation, “Public-Private Partnerships: Stimulating Innovation in the Space Sector,” <https://aerospace.org/sites/default/files/2018-06/Partnerships_Rev_5-4-18.pdf//ZW>]

The space economy, once the sole domain of wealthy countries, has rapidly transitioned to a complex ecosystem of public and private entities. Along the way, government and commercial sectors have learned by doing, recognizing and incorporating key successes and lessons learned from past partnerships. Stakeholders must sort through a myriad of complexities, conflicts, and contingencies to shape an acceptable agreement. Most stakeholders recognize that this process is more art than science. Yet there is potential to achieve greater efficiency without sacrificing transparency and accountability by utilizing a decision framework supported by a broad understanding of past experiences in multiple sectors. As the space sector engages in more P3s, more lessons will emerge as partners strategize, plan, and implement. In the meantime, the following lessons, from the case studies discussed above, should continue to resonate with future P3 arrangements: • The government partner must conduct a comprehensive review of a commercial partner’s business plan including market projections, market risk, and related cost projections. These factors may impact the ability to reliably deliver on time and within budget. Avoid business models that are overly optimistic or uncertain. • Create a shared vision among stakeholders. • Establish contingencies for changing requirements. Strategically leverage seed money for private sector development and encourage healthy competition by selecting multiple partners. • Use the partnership to incentivize industry to meet the more stringent demands of the government partner. • Scale contracts to the mission’s longevity and extended success. Be wary of commitments that are longer than technology refresh or capital reinvestment cycles. • Use success to fuel incremental growth and to build longer term trusted partnerships with commercial sector partners. • Carefully structure technical and financial milestones and measure success criteria for meeting milestones, including adjusting payment schedules to reflect any slippage. • Optimize value through shared data agreements between the public and private partners – focusing on a range of intended applications and niche markets. P3s will continue to test traditional approaches to space acquisition and operations. They can demonstrate significant advantages such as improving delivery schedules, quality of service, and innovation. Capitalintensive P3s will continue to experience successes and failures as both the public and private sector become more adept at crafting optimal arrangements. The future also holds great promise for public-private datasharing models as this type of arrangement will begin to spur innovation and extract the most utility from space-derived data products.

### Solvency---Ethical AI

#### Engaging NATO with the public-private sector solves ethical AI.

Michèle Flournoy and Anshu Roy 06-29-22 [Michèle Fournoy  is former US Undersecretary of Defense for Policy and an advisor to Rhombus, Dr. Anshu Roy is a Life Member of the Council on Foreign Relations and CEO of Rhombus, Just Security, “NATO Must Tackle Digital Authoritarianism,” https://www.justsecurity.org/82139/nato-must-tackle-digital-authoritarianism///ZW]

NATO leaders are gathered in Madrid this week to mark the reinvigoration of the transatlantic alliance and to discuss its ongoing challenges. After the fall of the Soviet Union, some dismissed NATO as a relic. Vladimir Putin’s brutal and unjustified war against Ukraine to expand Russia’s sphere of influence and reclaim its former glory stands as a stark reminder that hegemonic fantasies backed by brute force remain a threat to the international order, even in the 21st century. In response to Putin’s aggression, NATO has recovered its sense of purpose and relevance. It is also learning some important lessons regarding the future nature of warfare, from the criticality of adaptive leadership and robust logistics to the importance of asymmetric approaches. One of the most crucial lessons is that information dominance is essential, especially when confronting authoritarian powers like a revanchist Russia or a rising China who are willing to manufacture “facts” and create false narratives in order to undermine the political will and unity of their adversaries. As we look to the future, NATO must ask itself: How can we strengthen post-Westphalian institutions for a Wiki-world? In the last century, the United States and our allies sacrificed lives and treasure to defend the liberal world order, vanquishing the Axis Powers in World War II and Soviet Communism in the Cold War. In this century, traditional reliance on kinetic force is not enough. The ability to control, process, disseminate and protect information is critical. Malign actors are investing in a host of digital technologies without any restraint or regulation, preparing for the day when artificial intelligence (AI) becomes a dominant force on the battlefield. Digital authoritarianism – using technology for disinformation, ubiquitous surveillance and oppression of populations at home, and coercion abroad – is not the way of democracies, nor can it ever become our way. Instead, we need to reinvent our alliances and our own frameworks for information dominance consistent with our values. A coalition of like-minded nations could shape international technical and ethical standards, promote alignment on technology export controls, increase AI talent exchanges and technology investment, and importantly, facilitate cross-border data sharing. Creating an Artificial Intelligence Network in collaboration with our allies shouldn’t be just a hortatory statement or a commitment to compete on this turf with actors who don’t share our values. Instead, establishing information dominance through establishing such a network should be a strategic imperative. We have strengths, as do our allies, that authoritarian powers can only dream of, starting with free and open institutions that generate creativity and innovation across all intellectual and military disciplines. We can fully engage allied research universities and private sector companies to accelerate the development and integration of ethical AI that will give us an edge in everything from predictive warning of crises to better, faster human decision-making. For years, we’ve been fixated on whether countries are meeting their commitments under NATO to spend 2% of their GDP on defense. While more and more allies are meeting this goal, particularly in the wake of Putin’s aggression in the heart of Europe, the more provocative and consequential question for the long term is: Are we, together, investing in the development of the right new technologies and concepts? And are we adopting them with adequate speed and scale to be able to deter and, if necessary, defeat future aggression? The United States invested $4 billion in government-led, unclassified AI-related R&D in 2019 alone and remains the leading destination for global AI investments. Counting the private sector, America’s annual investment in AI is over $40 billion, with more than 2,000 American AI firms, including startups and large private companies. But making AI a strategic priority for NATO would be an enormous force multiplier. To date, Europe has lagged behind in AI. The MIT Sloan Management Review surveyed cross-industry AI practices and found 97% of Chinese companies have a strategy for AI, compared with just 62% of their European counterparts. Putting AI at the heart of the NATO Alliance could be a catalyst to addressing Europe’s growing AI gap. It could also create valuable synergies with U.S. efforts. After all, this is the playbook that won the Cold War: creating public-private synergy and bringing a network of trusted allies with shared values and tremendous talent and intellectual capacity into direct partnership with the innovation and creativity of America’s entrepreneurial centers and our capital markets. Alliances are about more than talking points or traditions–their value comes from what they can do now to shape a better future for us all. In the case of NATO, that means shaping a dynamic security environment in a period of intensifying great power competition and profound technological disruption. If NATO wants to stay relevant and be prepared for a very different future, it is time to modernize the alliance by working with allies today to triumph with tomorrow’s technology. That’s a conversation that should be front and center in Madrid.

### Solvency---Cyber

#### Collaboration is key to promoting good norms in cyberspace.

Eugenia Lostri, James Andrew Lewis, and Georgia Wood 03-22-22 [Eugenia Lostri is an associate fellow with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C. James Andrew Lewis is senior vice president and director of the CSIS Strategic Technologies Program. Georgia Wood is a program coordinator and research assistant with the CSIS Strategic Technologies Program, CSIS, “A Shared Responsibility: Public-Private Cooperation or Cybersecurity,” https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity//ZW]

**9. Expand Enforcement Cooperation with Allies** Cybersecurity is becoming a key part of the foreign policy agenda. To continue progress, participants believed that the United States, its allies, and partners should pursue the implementation of international norms for cyberspace to enhance accountability and responsible action. Supporting and promoting norms of responsible behavior and international law should be a priority, as well as raising the profile and stressing the urgency in diplomatic spheres. Collaboration between national CERTs during an incident was found to be valuable by many of the participants from global companies, who drew on resources in more than their home country. A global company will have relationships with several national CERTs. Support and communication from more experienced CERTs can make a big difference for smaller company teams, who may be dealing with an overwhelming workload. Another area participants believed would be useful to expanding collaboration is the arrest of bad actors. Some participants called attention to the FBI legal attachés in other countries. In a related vein, in October 2021, the United States convened the Counter Ransomware Initiative, which included representatives from 30 countries and the European Union to discuss the security threat posed by ransomware. One of the discussion points was, precisely, how to reinforce “timely and consistent collaboration across law enforcement, national security authorities, cybersecurity agencies, and financial intelligence units,” recognizing the transnational nature of the threat to improving enforcement.

### Solvency---Deterrence

#### Public-private partnerships solve deterrence.

John Allen et al 12-14-21 [General John Allen, President of Brookings and former Commander of NATO’s International Security Assistance Force in Afghanistan

Dr. Heiko Borchert, Director of Borchert Consulting & Research AG

Marcin Zaborowski, Policy Director of the Future of Security Programme, GLOBSEC, “Emerging technology, the geo-economic Achilles’ heel NATO needs to address,” https://www.globsec.org/news/emerging-technology-the-geo-economic-achilles-heel-nato-needs-to-address///ZW]

Emerging technologies are the geo-economics Achilles heel NATO needs to address to deter aggressors, write General John Allen, Heiko Borchert and Marcin Zaborowski. To ensure NATO’s relevance and to keep “our people safe”, the Alliance “must continue to strengthen and modernize our deterrence and defence,” NATO Secretary-General Jens Stoltenberg said at the Riga Summit on 30 November 2021. Innovation plays a critical role in modernizing armed forces amid a complex strategic environment. To this purpose, Stoltenberg unveiled the Defence Innovation Accelerator for the North Atlantic (DIANA) on 22 October 2021. DIANA shall bring defence and commercial companies together with military users to develop novel solutions that meet the needs of the future battlefield. He also launched the NATO Innovation Fund to invest up to €1bn to support innovators developing emerging technologies. The announcement comes at a time when the Alliance is working on a new Strategic Concept. Innovation will be key to preserving NATO’s edge, as the Secretary-General pointed out in his 2030 food for thought paper. Although NATO is a potent defence organization, emphasis on emerging technologies reveals its Achilles’ heel. Artificial intelligence, autonomy, biotechnology, quantum technology, and other technologies are at the heart of geo-economic competition. Geoeconomic competition unfolds around the projection of economic power within and across the domains of land, air, sea, space, and cyberspace to achieve political goals. Today’s geoeconomic dynamic defines winning business models amid a growing dichotomy between market-driven and state-driven nations. It aims to set the rules, principles, and standards that guide economic activities and access to and ownership of emerging technologies. NATO’s current emphasis on emerging technologies with defence and commercial applications risks making the Alliance subject to this new geoeconomic dynamic. This dynamic can undermine NATO’s innovation agenda and endanger its strategic edge. Therefore, NATO needs to respond. First, NATO needs to embrace the realities of economic security seriously. This call flows logically from Article 2 of the North Atlantic Treaty, encouraging allies’ economic collaborations. In our view, economic security combines national security and economic policy with technology and innovation policy to identify economic disruptions. It also prevents these disruptions from arising and strengthens a coping capacity to deal with economic emergencies. Economic security requires allies, for example, to engage on defence-critical standards, advancing transparency for defence supply chains, and considering the interplay between technology development, foreign direct investment, and export control. Therefore, the new Strategic Concept should incorporate economic security as an essential element. Second, economic security requires NATO to shape mindsets about defence investments and sustainability. Already today, defence companies face financial challenges as banks cancel bank accounts or refrain from covering export risks. The emphasis on environmental, social, and governance criteria (ESG) that increasingly shapes and determines financial investments will reinforce these problems as defence is considered toxic. But a narrow interpretation of ESG that considers defence incompatible with the world view underpinning ESG is detrimental to NATO’s ambition to invest in companies. It also means other investors will likely shy away from investing in the same companies. Therefore, the Alliance needs to step up activities with the European Commission, which works on a classification system to identify ESG-compliant activities, to make defence investments compatible. Third, business is the first line of defence in a geoeconomic world, and NATO needs a platform to discuss geoeconomics with business. Today, the NATO Industry Forum is the leading gathering to address defence industrial matters with defence companies. However, the emphasis on emerging technologies underlines the importance of non-defence companies. Therefore, NATO should envisage a new special format of the North Atlantic Council to meet with the NATO Industry Forum members – and possibly also the European Commission – to allow state and corporate leaders to jointly engage on the proposed economic security agenda. Fourth, strategic-level public-private dialogue also breathes new life into deepening cooperation with the private sector. NATO should become an early adopter of the solutions developed with allied money. Making NATO the launch customer sends important market signals and provides companies with an initial track record confirming the relevance of their solutions. In addition, the Alliance should step up efforts to incorporate business into military operations. Logistics companies already play a crucial role, and traditional defence businesses provide frontline support. The next stage comes with closely integrating digital companies to leverage their contribution. But for non-defence companies to provide frontline support, NATO not only needs the right mindset, but the Alliance also needs to think about incentives such as covering personnel risks on overseas deployments. Finally, NATO’s ability to stimulate innovation and ensure economic security also depends on how it does business. Critically, NATO needs to strive for a mission and capabilities-based innovation portfolio that maximises the value of allied money. NATO may take a page from the financial services industry and use a real options approach to manage technological risk and drive technology development. This approach prices technology building blocks like financial options, advances risk mitigation, speeds up technology adoption and gives force planners and developers more leeway to maximise input and output. In addition, NATO should offer strategic hedging solutions for defence critical raw materials by combining corporate demand estimates with AI-based insights on financial and raw material markets. This will facilitate optimal, company-tailored hedging strategies to mitigate the corporate security of supply and price risks. Overall, NATO’s relevance in the 21st century remains tackling defence challenges in a new strategic environment, increasingly defined by emerging and rapidly changing technologies and the profoundly important role of the private sector. To this purpose, NATO has embraced innovation and emerging technologies. This step, however, makes NATO subject to a new geoeconomic dynamic that unfolds around competition for standards, business models, technologies, and supply chains. This requires NATO to make economic security a core element of its new Strategic Concept to ensure NATO’s edge. In turn, this will provide a sound basis for expanded cooperation with the European Union, and make NATO an esteemed partner of the new Transatlantic Trade and Technology Council, the new body set up to enhance the EU-U.S. technology, economic, and trade partnership.

### Solvency---Interoperability

#### Solves interoperability.

Rose Gottemoeller et al. 06-26-2022 [**Gottemoeller** served as the Secretary General of NATO from 2016 to 2019. Prior to NATO, she served as the Under Secretary for Arms Control and International Security at the U.S. Department of State. Gottemoeller was also the chief U.S. negotiator of the New Strategic Arms Reduction Treaty (New START) with the Russian Federation ***Maj. Kathryn Hedgecock***, U.S. Army, is an assistant professor in the Department of Social Sciences at West Point. She holds a Ph.D. and M.A. from Stanford University in Political Science. ***Maj. Justin Magula***, U.S. Army, is an Army strategist in the Strategic Landpower and Futures Group at the U.S. Army War College. ***Paul Poast*** is an associate professor in the Department of Political Science at the University of Chicago. Paul received his PhD from the University of Michigan, Defense Studies, “Engaging with emerged and emerging domains: cyber, space, and technology in the 2022 NATO strategic concept,” https://www.tandfonline.com/doi/full/10.1080/14702436.2022.2082955//ZW]

In discussions of Cooperative Security, NATO must distinguish between emerged and emerging technologies, categorizing cyber operations as an emerged technology (Kosal 2022). NATO should strive to remain on the “bleeding edge” of scientific development by continuing to establish cooperative partnerships with private industry, including support of start-up organizations to enhance NATO’s competitive edge. NATO can enhance collective defense among member states by fostering partnerships through science diplomacy oriented toward emerging threats (Breedlove and Kosal 2019). Finally, NATO must mitigate risks associated with interoperable emerging technologies that rely on the cyber and space domains.

### Solvency---Ethical Tech

#### Inclusion of private actors solves downside risks

Nadja El Fertasi 06-22-2019 [El Fertasi has built a career path in NATO over the past seventeen years taking on a variety of posts in different fields within large multinational NATO institutions. She holds a Master’s degree in International relations from the University of Cambridge and is an alumna of the NATO-wide Executive Development Program, Information and Security, “Why Digital Ecosystems of Civil-Military Partnerships Are a Game Changer for International Security and Defence,” https://procon.bg/system/files/4202\_elfertasi\_digital\_ecosystems.pdf//ZW]

Fostering understanding, sharing best practices and lessons learned through dialogue is crucial for keeping pace with digital transformation on both sides of the Atlantic. This forum, focused on digital transformation at large in the defence sector, can help identify problems which need collaborative approaches across the civil-military spectrum. Understanding the problem first from multiple angles will create a vision all stakeholders stand behind. Establishing this dialogue to foster this shared understanding is one of the essential steps for building inclusive public-private partnerships in keeping pace with the challenges of digital disruption. NATO has excellent resources that take innovation to the next level fit for the defence sector. The NATO Industry Advisory Group 21 is the primary forum that serves as an industry advisory hub for NATO and has a transatlantic focus. Building on this forum and expanding its focus from information technology to technology at large to include all five domains of air, maritime, land, space, and cyber will reinvigorate transatlantic-public private partnerships in the digital age. Focusing on disruptive technology that is driving digital transformation in the current era is a necessity. However, the dark side of technology does not recognise civil-military boundaries; thus, involving non-traditional actors is crucial. Rethinking military doctrine and civil-military cooperation in the digital age to maintain information superiority is what will provide ultimate security. Forging partnerships within inhouse NATO expertise (e.g., Allied Command Transformation, Science and Technology Organization, NATO Communications and Information Agency) with the civil sector to include prime contractors, small and medium enterprise, startups, academia and research and development bodies will bring civil-military cooperation into the digital age. A forum for developing a shared understanding on what disruptive technology means for different member states on both sides of the Atlantic will set the scene for bridging the widening innovation gap. Anderson and Townsend argue that disruptive technologies have different meanings in the United States and Europe. 22 Add to that the innovation gap both across the Atlantic and within Europe between various member states, understanding how digital transformation impacts the different security landscapes and interests are paramount for closing this gap. A final aspect to consider is to include all institutional stakeholders from legal, finance, military officers – both users and commanders, the full spectrum of the industry from prime contractors to start-ups, and other non-traditional stakeholders. In particular seen from the recent implementation of Europe’s GDPR regulation which impacts transatlantic digital cooperation. 23 A frank and open dialogue on moving forward in ensuring Europe’s innovation culture does not fall behind in the bigger world scene is warranted. By establishing this dialogue, institutional blindness across the Alliance will diminish, and more focus on finding opportunities within existing bureaucracies will prevail.

### Solvency---Complexity

#### PPPs are key to address complexity.

Nadja El Fertasi 06-22-2019 [El Fertasi has built a career path in NATO over the past seventeen years taking on a variety of posts in different fields within large multinational NATO institutions. She holds a Master’s degree in International relations from the University of Cambridge and is an alumna of the NATO-wide Executive Development Program, Information and Security, “Why Digital Ecosystems of Civil-Military Partnerships Are a Game Changer for International Security and Defence,” https://procon.bg/system/files/4202\_elfertasi\_digital\_ecosystems.pdf//ZW]

Digital Ecosystems of Civil-Military Partnerships are no Longer a Luxury, but a Necessity Working with traditional and non-traditional partners, training military leaders and soldiers to become digitally literate is essential in an era marked by information warfare for superiority, and where data is the new oil and a strategic resource. Numerous actors in the defence and security sector have been arguing for a digital approach in protecting data while fully harnessing its full potential in bringing civil-military partnerships to the next level. During his speech at the NATO Science and Technology Organization conference, NATO’s Supreme Allied Commander for Transformation General Denis Mercier argued that homogenous partnerships are part of the past. 6 Traditional and homogeneous partnerships are no longer keeping us safe from the dark side of technology as peer state competitors, and non-state actors tap into cutting-edge technology at low cost posing highly complex challenges to both military and civil infrastructures. Technology has become the world’s nervous system making networks across the globe increasingly vulnerable to a vast array of threats. Bringing in experts from a broad spectrum of disciplines and across generations will help develop innovative and sustainable solutions to technology threats in an era where information superiority prevails. The Case of Public-Private Partnerships in the United States The United States has understood the value of establishing public-private partnerships with tech giants to address some of the most complex security challenges digital transformation brings. In his speech to Stanford University, former United States Secretary of Defense Ashton Carter emphasized that a strong partnership between military strategists and technologies would establish a strong pact in an era marked by digital transformation. He added: The same Internet that enables Wikipedia also allows terrorists to learn how to build a bomb. And the same technologies we use to target cruise missiles and jam enemy air defenses can be used against our own forces – and they’re now available to the highest bidder. This is why, he said, the Pentagon must rebuild the bridge between Washington and Silicon Valley. “Renewing our partnership is the only way we can do this right.”

### Solvency---Demoracy

#### Public private partnerships with NATO bolster democratic institutions.

Martin Banks 2019 [Writing for EU Political Report, EU Political Report, “How to Strengthen Public-Private Cooperation in Hybrid War, https://www.eupoliticalreport.eu/how-to-strengthen-public-private-cooperation-in-hybrid-war///ZW]

Western nations need to build closer partnerships with the private sector to sharpen NATO and the European Union responses to hybrid security threats, participants at a unique day-long exercise concluded on Thursday. “Hybrid warfare is now real warfare,” Jamie Shea, Senior Fellow at Friends of Europe and former Deputy Assistant General at NATO. “This is an opportunity for the private sector and government to solve the problems.” Shea spoke during the tabletop exercise “Strengthening Public-Private Cooperation in Hybrid Crises” organized by Friends of Europe in partnership with the Finnish Presidency to the European Union and the United States European Command (EUCOM). The event drew over three dozen senior officials and security experts from NATO, European institutions, national authorities and private companies to examine how they can build society-wide resilience to hybrid challenges. Participants underscored the need to build trust that creates a “co-working” space for private and public players to ensure seamless cooperation in the event of a crisis. “Partnership with the private sector, has to more than just cooperation,” said a lawmaker from one NATO ally. “It should be about formulating policy together, not just cooperating when you have a problem,” they added, pointing out that the private sector is often the target of hybrid attacks as well as a solution provider. The exercise was based on responses to a fictional scenarios that included the high-jacking of a ship loaded with liquified natural gas which terrorists threaten to explode in a crowded port city; cyber-attacks that shut down banking services in a European Union country ahead of sensitive elections; and the mysterious severing of undersea cables linking the country to the rest of the EU. Among the ideas, participants emphasized the need for better intelligence sharing to ensure relevant policy makers are fully informed of hybrid risks; the importance of greater international cooperation between law-enforcement and civil protection services to match that among the military; for pro-active media strategies to keep citizens informed and counter fake news during a crisis; and outreach to all sectors of society to counter hostile efforts to undermine faith in democratic institutions. “If we adopt resilience it will serve us for all sorts of scenarios, so it’s a win-win situation,” Shea concluded. The exercise, which was also conducted with the support of Facebook, is Friends of Europe’s newest flagship project.

#### PPPs work--- sony hack proves.

Cheryl Pellerin 11-16-2016 [Writing for Department of Defense, Department of Defense, “Cybercom Commander: Public-Private Partnership Needed for Cybersecurity,” https://www.defense.gov/News/News-Stories/Article/Article/1006807/cybercom-commander-public-private-partnerships-needed-for-cybersecurity///ZW]

The public-private cybersecurity partnership between private companies and U.S. Cyber Command and other federal agencies has been uneven so far despite some fledgling success, but collaboration is critical given growing threats to everyone from cyberspace, the commander of U.S. Cyber Command said here yesterday. Navy Adm. Mike S. Rogers, who is also director of the National Security Agency, spoke during the Wall Street Journal’s CEO Council annual meeting on the fight for global security in an era of borderless wars. On the government’s ability to help industry during major cyberattacks, Rogers said it’s unrealistic to expect the private sector alone to withstand the onslaught of activity that is being directed against them by nation-states and other actors. “Likewise,” the admiral added, “I don't think it's realistic to say the government's just going to do this [by itself] because the challenge with the government doing it is, if you want me to defend something I can't … defend a network if I ... don't have access to that network structure,” a level of outside access the private sector has resisted. **Critical Success** An exception to this was Sony Corporation after a 2014 Sony Pictures Entertainment hack of confidential data sponsored by North Korea. Rogers said that a positive aspect of the hack was great collaboration among a private company, the private-sector computer network expertise that Sony brought in and federal agencies. “They knew they were dealing with something [after the hack] so they went out and hired expertise and capability from within the private sector,” the admiral said. “They then came to the conclusion that this was something bigger than they had initially thought so they reached out to the government. I give them big kudos for that.” Sony officials were “very up front” when they approached the government, he added, saying they asked for help to understand what happened and to make sure it didn’t happen again. **Providing Value** “We said, if you want us to provide value and insight we need full access to your network and your data,” Rogers recalled, adding, “They had no issue at all, just insure that you inform us of what you're doing, why you're doing it and exactly what you're doing and you stick to that.” It “worked out great,” Rogers said, and there was good information flow between Sony and the U.S. government response team, which consisted mainly of Cybercom, NSA, the FBI and the Department of Homeland Security. “One of the reasons why the partnership is so important -- using NSA resources to monitor and guard U.S. networks -- that's not our mission,” Rogers said in March 2015 in testimony before the House Armed Services Committee on cyber operations, “and it's against the law … but on the other hand, I do want to create a partnership where we're able to share information with each other.” The FBI was designated as the lead agency, Rogers said, “and the FBI turns to NSA and says, ‘We could use your analytic help, will you partner with us in working with Sony?’” The admiral said Sony cooperated completely with the government during the investigation. **Significant Calamity** Rogers said that as director of NSA and commander of Cybercom, the agreement he always reaches with whoever they’re working with is that neither agency will use the data they gain for anything other than the exact purpose they’ve discussed. “I don't want it to get to the point where it takes some significant calamity to drive us to the conclusion that we've got to do something different than what we're doing now,” the admiral added. During Rogers’ remarks, the audience of chief executive officers participated an instant poll was taken on the question: Do you trust the government enough with your information to work with it during a cyberattack? The choices were: a) absolutely, b) only if my company is attacked, or c) never. The result was that 56 percent said they “absolutely” trusted the government enough to work with them, 34 percent said only if their company was attacked, and 9 percent said “never.” For Rogers, this was a positive result. “Overall that's pretty good,” he said. “Less than 10 percent of you said that there were no circumstances under which [you] would consider doing this. From my perspective that's a broad positive -- that means there's a willingness among 91 percent of you to have some form of dialog and to potentially look at [partnering with the government on cybersecurity] as a possibility.”

### INB

#### Emphasizing private innovation is key to NATO readiness and interoperability.

Aaron Bazin and Dominika Kunertova 2017 [Lt. Col. Aaron Bazin, refined these ideas PsyD, is a transitioning U.S. Army officer, Functional Area 59 (strategist). He holds a doctorate in psychology, specializing in mediation and conflict resolution. He has over twenty years of experience including service with NATO and the U.S. Army Central Command, Dominika Kunertova is a PhD candidate in the Department of Political Science at the Université de Montréal, Quebec, Canada. She holds a BA in political science from Comenius University, Bratislava, Slovakia, and an MA in international relations from Charles University, Prague, Czech Republic, Army University Press, “An Alliance Divided? Five Factors That Could Fracture NATO,” https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2018/An-Alliance-Divided-Five-Factors-That-Could-Fracture-NATO///ZW]

Technology advances. The participants agreed that technology advances are important for NATO’s continued cohesion. Technology will constitute a significant intervening factor in how NATO nations maintain their cohesion in the future for three reasons. First, ever-evolving communication technology can facilitate the spread of risks coming from outside of the Alliance and exacerbate their negative effect. The examples that resonated the most during focus group sessions are information warfare and targeted propaganda against NATO nations. Internet communications technology creates infinite room for alternative media that distort reality, contribute to the emergence of populist and radical movements, and increase the danger of miscommunication among nations. Second, NATO risks losing the innovation game to the commercial defense industrial sector. In the future, private companies will continue to stay ahead of NATO in designing specifications and setting standards for platforms. This can have a major impact on readiness and interoperability among NATO nations if their innovation efforts (e.g., the U.S. Third Offset Strategy) do not materialize.31

#### Military-to-military cooperation harms innovation

Nadja El Fertasi 06-22-2019 [El Fertasi has built a career path in NATO over the past seventeen years taking on a variety of posts in different fields within large multinational NATO institutions. She holds a Master’s degree in International relations from the University of Cambridge and is an alumna of the NATO-wide Executive Development Program, Information and Security, “Why Digital Ecosystems of Civil-Military Partnerships Are a Game Changer for International Security and Defence,” https://procon.bg/system/files/4202\_elfertasi\_digital\_ecosystems.pdf//ZW]

The Challenge of Military Adaptation To keep the military edge and prevail in future operations, NATO forces must continually evolve, adapt and innovate and be credible, networked, aware, agile and resilient. 12 Under NATO’s renewed collective defence posture, there is a greater emphasis on static versus deployable presence. The efforts underway to implement an adapted NATO Command Structure to achieve NATO’s level of ambition are grand. However, what is even more daunting is the cultural change needed within a homogeneous culture to embrace non-traditional ways of working. For example, high readiness and deployment of forces within the needed timeframe remain critical issues for years to come. Challenges and gaps in interoperability, cyber, logistics and hybrid warfare which became prevalent during NATO’s enhanced and tailored forward presence require comprehensive and inclusive partnerships beyond the military. This requires tapping into the human potential across disciplines and all backgrounds within the civil-military spectrum.

#### The perm stovepipes innovation in the military

Rose Gottemoeller et al. 06-26-2022 [**Gottemoeller** served as the Secretary General of NATO from 2016 to 2019. Prior to NATO, she served as the Under Secretary for Arms Control and International Security at the U.S. Department of State. Gottemoeller was also the chief U.S. negotiator of the New Strategic Arms Reduction Treaty (New START) with the Russian Federation ***Maj. Kathryn Hedgecock***, U.S. Army, is an assistant professor in the Department of Social Sciences at West Point. She holds a Ph.D. and M.A. from Stanford University in Political Science. ***Maj. Justin Magula***, U.S. Army, is an Army strategist in the Strategic Landpower and Futures Group at the U.S. Army War College. ***Paul Poast*** is an associate professor in the Department of Political Science at the University of Chicago. Paul received his PhD from the University of Michigan, Defense Studies, “Engaging with emerged and emerging domains: cyber, space, and technology in the 2022 NATO strategic concept,” https://www.tandfonline.com/doi/full/10.1080/14702436.2022.2082955//ZW]

The cyber and space domains have often been interpreted as public commons. As a result, these commons are difficult to govern and serve as the intersection of public and private actors. NATO must seek to lead cooperation within the Alliance, across partnership states, and with private actors to maintain a scientific edge (Rugolo and Monic 2022). NATO currently supports the Industry Cyber Partnership to improve Allies’ network security and increase resilience. This industry partnership must be replicated in a NATO Industry Emerging Technology Partnership, to facilitate a competitive edge in capabilities that are on the horizon or not fully realized in the operational security environment. The agreement to establish Defense Innovation Accelerator for the North Atlantic (DIANA) for civil-military cooperation at the 2021 Brussels Summit, is a step in the right direction. Once established, cooperation must also be facilitated across partnership hubs within NATO to prevent stove piping of innovation. Additionally, it is critical that these innovation centers encourage partnerships across the entire spectrum of private industry, from startups and garage innovators to large scale private corporations with extensive scale research and development (Kosal 2022). Finally, intra-Alliance cooperation requires intelligence sharing and capability development among member states to ensure that the Alliance continues to meet the challenges of the strategic environment. One example of intra-Alliance cooperation that compliments NATO’s efforts is the European Union’s initiatives to bolster cybersecurity. The European Union Agency for Cybersecurity’s efforts to improve capacity, cooperation, and a whole-of-society approach to cybersecurity ultimately bolster NATO’s deterrence by denial by hardening the attack surface of Europe.

### AT International Fiat

#### No--- the cp has the USfg enter a public-private partnership with relevant corporations--- funding is provided by the DIANA fund and the mandate is carried out by cooperation between the PPP and nato.

#### It’s legal--- US Code.

US Code Title 10 [From Title 10-ARMED FORCES Subtitle A-General Military Law PART II-PERSONNEL, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section1501a&num=0&edition=prelim//ZW]

§1501a. Public-private partnerships; other forms of support (a) Public-private Partnerships.-The Secretary of Defense may enter into arrangements known as public-private partnerships with appropriate entities outside the Government for the purposes of facilitating the activities of the designated Defense Agency. The Secretary may only partner with foreign governments or foreign entities with the concurrence of the Secretary of State. Any such arrangement shall be entered into in accordance with authorities provided under this section or any other authority otherwise available to the Secretary. Regulations prescribed under subsection (f)(1) shall include provisions for the establishment and implementation of such partnerships. An employee of an entity outside the Government that has entered into a public-private partnership, cooperative agreement, or a grant arrangement with, or in direct support of, the designated Defense Agency under this section shall be considered to be an employee of the Federal Government by reason of participation in such partnership, cooperative agreement, or grant, only for the purposes of section 552a of title 5 (relating to maintenance of records on individuals)

### AT PDB

#### Companies agree to partnership--- but don’t like government overreach. The perm means they say no.

Edward Segal 07-01-2022 [Senior Contributor for Forbes, Forbes, “What Business Leaders Need To Know About NATO’s New Cyber Initiative,” https://www.forbes.com/sites/edwardsegal/2022/07/01/what-business-leaders-need-to-know-about-natos-new-cyber-initiative/?sh=280252f33764//ZW]

A new initiative announced by NATO at its summit this week in Madrid has important implications for business leaders who are concerned about cyberattacks. The multinational organization said it will launch a rapid response force that will ramp up collaborations with military and civilian organizations to help meet cyber threats. As important as it is to protect against and respond to cyber threats, the plan comes with built-in challenges and limitations. Strengthening Cyber Defenses “We are confronted by cyber, space, hybrid and other asymmetric threats, and by the malicious use of emerging and disruptive technologies,” NATO said in a statement. “We face systemic competition from those, including the People’s Republic of China, who challenge our interests, security, and values and seek to undermine the rules-based international order.” “We will significantly strengthen our cyber defenses through enhanced civil-military cooperation,” the declaration says. “We will also expand partnership with industry. Allies have decided, on a voluntary basis and using national assets, to build and exercise a virtual rapid response cyber capability to respond to significant malicious cyber activities.” Challenges “Most of those in the cyber world are excited about this possibility but some challenges face it. First, it is all voluntary so countries and industries will have to want to actually do it. Second, each country may do something different so it could be patchwork in its establishment,” crisis management expert Baruch Labunski, CEO of Rank Secure said in an email interview. “Finally, the joint effort of civilian industry and the military can be commendable or dangerous. It depends on your point of view and how one looks at government overreach,” he observed. Taking Responsibility NATO’s new program does not take the pressure off companies and organizations to protect themselves from cyberattacks. “Cybersecurity teams must take responsibility as information warfare continues to become part of the rapidly evolving threat landscape,” Wasim Khaled, co-founder and CEO of Blackbird.AI said in an email. “These new risks are driven by a new breed of threat actors who exploit digital media to drive harmful narratives that can [impact] organizations, employees, and executives using sophisticated tradecraft and technologies." Hybrid Warfare "In today's threat landscape, military adversaries and threat actors are combining cyber, information and kinetic attacks as a form of hybrid warfare that is highly effective when coordinated,” Khaled said. “The new NATO cyber rapid reaction force will help countries against cyberattacks that are designed to intimidate and disrupt an entire nation,” he observed. ‘No Surprise’ At least one cybersecurity expert was not surprised by NATO’s announcement. “For those that work in the field of cybersecurity, NATO’s new strategy comes as no surprise. As we suspected and have now confirmed through the conflict in Ukraine, cyberspace is a critical dimension of operations in modern warfare,” Robert Stines, a partner in the Litigation Practice Group at Freeborn & Peters and a cybersecurity advisor said in a statement. “We have also learned from past events that cyber threats tend to detrimentally impact the private sector,” he noted. To Be Determined “While we know very little about the scope of NATO’s new strategy, the pledge to work with the private sector to counter threats is very encouraging. Of course, the question becomes how does the private sector benefit from NATO’s new commitment,” Stines said. “It will also be interesting to see how NATO plans …to bring together governments, the private sector, and academia to bolster NATO’s technological edge. I suspect that America’s technology giants (Alphabet, Meta, Microsoft) will have a role in the Accelerator,” he concluded. 3 Key Cyber Trends Preventing and responding to cyberattacks continues to be a top priority and business leaders should be aware of three key related trends, according to Khaled. He said the trends include: Convergence “Convergence between information operations and traditional cyberattacks will continue to increase. Modern cybersecurity companies will integrate specialized information operations technology and fuse these capabilities with their existing cyber threat platforms.” Attacks On Supply Chains “Supply chain attacks will be on the rise due to ongoing economic shortages and disruptions through ransomware and other means in these critical times which could consist of holding victim’s data hostage, leaking and publicizing breaches, and attacking vendor supply chains.” Ransomware “Modern ransomware extortion will continue to proliferate across traditional enterprise environments. The market size for offensive skills has grown incredibly due to the potential payout size of cryptocurrency breaches that can exceed $100M on a single intrusion.”

#### Public investment crowds out private.

Mohammad Taslim Uddin and Hasina Akter 2021 [Uddin is of the University of Chittagong, Bangladesh, Atker is of the International Islamic University Chittagong, Bangladesh, Journal of Developing Areas Winter 2021, Volume 55 No. 1, “Macroeconomic rates of return of investment in public-private partnerships: evidence from South Asian region,” https://muse.jhu.edu/article/766453/pdf//ZW]

Public investment creates a crowding-out effect on both private and PPP investment. In the presence of a positive shock in public investment, the IRFs show a positive impact on both private investment and 𝐺𝐷𝑃, with a fluctuation around zero in the time path of 𝐼𝑃𝑃𝑃. However, the output elasticity of public investment is negative; the total RoR is positive and large in magnitude, possibly because in the presence of a shock in public investment the response from private investment and investment in PPP leads to an increase in output. Finally, private investment crowds-in both PPP and public investment. The output elasticity of private investment is found to be positive. The partial RoR of private investment is positive, while its total RoR is found to be negative.

### AT PDCP

#### Severs security cooperation

#### A---It’s exclusively military-to-military

Van Eerden 20, Captain (James, “Seeking Alpha in the Security Cooperation Enterprise A New Approach to Assessments and Evaluations,” Journal of Advanced Military Studies, 11.1)//BB

The Fiscal Year (FY) 2019 President’s Budget: Security Cooperation Consolidated Budget Display outlines seven categories of security cooperation activity, including military-to-military engagements, support to operations, and humanitarian and assistance activities, among others.6 The security cooperation framework traditionally includes security assistance (SA), security force assistance (SFA), and some aspects of foreign internal defense (FID).7 In the context of this article, the term security cooperation refers primarily to military-to-military engagements, where the U.S. military engages in training partner forces under the auspices of Title 10 and Title 22 authorities.

#### Qualified experts agree

Finkelstein 10, PhD, Vice President of the CNA Corporation, an independent, non-profit research institution in Arlington, Virginia (David, “The Military Dimensions of U.S.-China Security Cooperation: Retrospective and Future Prospects,” *Center for Naval Analyses*, <https://apps.dtic.mil/sti/citations/ADA530755>)//BB

The United States and China have engaged in security cooperation on a variety of international issues since the normalization of relations in 1979. In fact, security cooperation began even before the formal establishment of state-to-state relations. We recall that during the height of the Cold War the two nations demonstrated that when a pressing and shared security concern in that case, the former Soviet Union presented itself, Washington and Beijing were capable of working together, extant differences notwithstanding. Security consultations and sometime security cooperation between the two countries continue today. But as the record of security cooperation is reviewed, one comes to the conclusion that, for the most part, U.S.-China security cooperation has been mainly of a political nature and operationalized at a high level of strategic policy coordination. Security cooperation between the two nations has been largely the purview of U.S. and Chinese civilian officials and diplomats, not generals and admirals. In other words, over the course of 30 years of relations, security cooperation between the defense-military establishments of the United States and China -- the uniformed services -- has been the exception rather than the rule. If a serious discussion about future security cooperation between the U.S. Navy and the PLA Navy is to take place -- a leitmotif of this series of conferences as described by the sponsors -- then some of the issues, challenges, and problems from the past need to be confronted even as we look over the horizon. For the purposes of this paper, security cooperation is defined as the two militaries working together to achieve a common objective -- not high-level visits, exchanges, port calls, or other activities that are mainly symbolic or representational in nature.

#### B---Resource dispersion. The counterplan provides resources to the domestic private sector not to foreign countries

Fenell 11, Captain, US Marine Corps, In Partial Fulfillment of the Requirements for the Degree MASTER OF ARTS in INTERNATIONAL STUDIES, at the UNIVERSITY OF SAN FRANCISCO (Nathan, “Security Cooperation Poorly Defined” December, <https://repository.usfca.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1020&context=thes>)//BB

Security cooperation is a compilation of financial, educational, and material resources, that at their foundation are supported by the United States, in particular the Department of Defense, and are used to support the peaceful development of democracies in foreign countries. The resources provided by the Department of Defense are available to foreign countries after the host nation requests the peaceful assistance of the U.S. military in response to systemic deficiencies in the bureaucratic management of a nation state or when a nation state recognizes that its military limitations prevent it from properly defending its geographic borders. The host nation’s request for support from the U.S. is typically an effort by the foreign country to develop its internal capacity to protect its people and limit internal or external threats. The security cooperation exercise Baltic Operation, held in Estonia, is an example of a foreign country using the resources 9 provided by the United States to improve its national defense capabilities in direct response to a perceived threat to its sovereign borders. In this scenario Estonia is attempting to develop its military capabilities and project an image of strength in an effort to maintain the freedom it earned, from Russia, at the conclusion of the Singing Revolution in 1992 and prevent a future Russian incursion across its borders. In contrast to this appropriate use and definition of security cooperation as a strategy to prevent conflict, the Obama Administration is using the term security cooperation as a way to define a national exit strategy from a two front war, a strategy that at its heart is based on the reconstruction of a damaged infrastructure. The false labeling of reconstruction operations as security cooperation is the foci of this thesis project.

## AFF

### PDCP

#### Security cooperation includes development of economic capabilities

MAJ Nicholas R. Simontis, 13 - U.S. Army School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas “SECURITY COOPERATION: AN OLD PRACTICE FOR NEW TIMES” <https://apps.dtic.mil/sti/pdfs/ADA589722.pdf>

How we deal with our adversaries is changing in response to these developments in the security environment. How we deal with our international allies and partners also should change. For many years, the term “security cooperation” referred to efforts by the Department of Defense (DOD) to promote U.S. security interests through the interaction with and development of friendly and allied security capabilities.2 This definition is evolving, however, as illustrated by recent strategic documents and statements by the President and Secretary of Defense.3 The term as used recently includes synchronized efforts by the whole-of-government to build the security capacity of U.S. friends and allies, including the development of economic and political capabilities. The most recent strategic guidance calls for increased emphasis on an interagency and interorganizational approach to building partner capacity and capability, focused on promoting stability and preventing conflict before it begins, all within a framework that emphasizes governance and rule of law. Put another way, recent strategic guidance advocates a whole-of-government approach as the means for translating national security objectives into the outcome of increased partner capacity. This change represents recognition that a wide variety of skill sets is necessary to address these changes in the security environment. Unfortunately, this change presents challenges for current security cooperation practices.

The current structure of security cooperation, that is, the infrastructure of government agencies that participate in security cooperation activities, does not readily support this new guidance. The current security cooperation organization originated in the aftermath of World War II, and continued to evolve through the Cold War. Although the Department of State (DOS) has responsibility for planning and executing security cooperation, the system primarily addresses the military component of security in terms of equipment and training. The DOD, under the auspices of the Defense Security Cooperation Agency (DSCA) executes these portions of U.S. Security cooperation endeavors, which constitute the preponderance of efforts, both in terms of labor and fund allocation. Furthermore, the DOD’s share has grown considerably in the past five years as Congress significantly increased funding authorities in order to facilitate stabilization in Iraq and Afghanistan.4 The key issue, then, is how to shift the emphasis from the Department of Defense to efforts shared among Defense, State, USAID, and other agencies as needed.

### PDB

#### The private sector and military can work together.

Kolinda Grabar-Kitarovíc 06-16-2022 [Former President of Croatia, Defense One, “NATO Must Ensure Defense and Civilian Industries Work Together,” https://www.defenseone.com/ideas/2022/06/nato-must-ensure-defense-and-civilian-industries-work-together/368250///ZW]

The internet, microwaves, and synthetic rubber came into our lives as products invented for military purposes. Even everyday things, such as undershirts and concentrated fruit juice were created to improve the combat readiness of armed forces. Though many people typically associate the military with war and suffering, this industry has been a source of incredible progress, producing inventions that made our lives longer, healthier, and easier. These days, innovation is likely to run the other way, with the military benefiting from inventions developed with private funding. A symbiotic relationship between military needs and human progress is not necessarily the default. Instead, it requires a well-oiled innovation ecosystem in which military and civilian industries share their expertise and knowledge with one another. NATO has recently announced several initiatives to build on past success, but more are needed—particularly as members increase their military funding. Virtually all alliance members are investing more in defense or are soon planning to do so. Germany, for example, declared that it would create a 100-billion-Euro fund and reach its 2% goal in 2022. Poland, which shares the longest EU border with Ukraine, has taken in more than 3.5 million Ukrainian refugees and promised to dedicate 3% of its GDP to defense. Croatia ramped up its defense investment to 2.3% of GDP. To ensure that this new investment spurs innovation and co-operation between military and civilian industries as well as academia, NATO announced in April the Defense Innovation Accelerator for the North Atlantic. DIANA will concentrate on deep technologies, including artificial intelligence, big-data processing, quantum-enabled technologies, biotechnology, novel materials, and outer space. In addition, 17 NATO nations have agreed to set up the world’s first multi-sovereign venture capital fund. It will invest 1 billion Euros in early-stage startups and other deep tech funds aligned with its strategic objectives. But NATO members need to do more to maintain their technological advantage over Russia and China, who are also increasing spending on military research and development. The trends make this clear. In 1960, the U.S. accounted for 69 percent of global R&D investments, with U.S. defense-related R&D accounting for no less than 36% of global spending. The bulk (65%) of U.S. investments in defense-related R&D was financed from the federal budget. However, by 2019, the U.S. share of global R&D fell to 30%, and the share of federal government investment in defense-related R&D fell from 65% to 21%, whereas the share of business investment in R&D has grown from 33% to 71%. This leaves no doubt that meaningful innovation is not possible without close co-operation with the private sector. As NATO prepares to adopt its next Strategic Concept at the summit in Madrid, it is essential that it focus on mechanisms that maintain its technological advantage. As part of GLOBSEC’s work at the Future Security and Defense Council, we have proposed several ideas to help promote innovation in the Alliance. We are convinced that NATO’s innovation ecosystem must integrate public and private sectors to ensure this edge.

### Solvency

#### The counterplan fails--- the government and private sector don’t trust each other.

Evelyn Farkas 08-11-2011 [Evelyn N. Farkas, Ph.D., Senior Advisor for Public-Private Partnership to the Supreme Allied Commander (SACEUR) and Commander, U.S. European Command, Atlantic Council, “Public-Private Collaboration in NATO,” https://www.atlanticcouncil.org/blogs/natosource/publicprivate-collaboration-in-nato///ZW]

From Evelyn Farkas, U.S. European Command: “Why should the public and private sectors collaborate today?” The answer? The complex challenges that we face around the world today often require skills and approaches beyond traditional military capabilities. Collaboration allows us to meet these challenges utilizing specific expertise found in the private sector. The private sector can provide agility, swift innovation, and a unique resource set. Together, government and private entities can reduce shared risks, minimize costs, and address mutual threats like terrorism, organized crime, cyber attacks, and climate change. The government gains access to the private sector’s expertise and resources, and private sector entities benefit from the information sharing involved in collaboration and the legitimacy gained from meeting complex challenges to provide for the greater good. . . . NATO adopted a comprehensive approach that recognized the need to build partnerships with non-military entities both inside and outside the government. With this in mind, in 2008, NATO launched the Building Integrity Initiative, which works with private NGOs like Transparency International, to reduce corruption in defense establishments in Europe and Afghanistan. . . . First, is the issue of trust. Neither sector likes to broadly share information about vulnerabilities. Corporations worry that it could lead to the public revelation of weaknesses and of sensitive intellectual property. The government is cautious about disclosing national security vulnerabilities to private entities that have international ownership or global interests and about safeguarding the privacy of U.S. citizens. And finally, there is the problem of how to institutionalize this collaboration. Because the responsibility for advancing public-private collaboration is so decentralized, optimization and coordination of efforts across the government has proven to be difficult.

### Impact Turn

#### Confronting China causes overstretch and escalation spirals.

Depetris 8-18-2020, fellow at Defense Priorities and a columnist at the Washington Examiner. (Daniel Depetris, "China isn't the Soviet Union, and the US needs to find a different way to compete", *Business Insider*, https://www.businessinsider.com/us-needs-to-find-different-way-to-compete-with-china-2020-8)

Unfortunately, simplifying China as a modern-day Soviet Union misdiagnoses the problem and leads to a faulty cure. Combatting Chinese power everywhere and anywhere will exhaust the US, deplete its resources and weaken US power over the long-term.

For nearly 30 years, the Washington foreign policy establishment has gotten used to the United States being the paramount power in the global system. But this is no longer the world we are living in.

While the US is still the world's largest military and economic power, China is a close second. Since the dawn of the century, the Chinese economy has increased from $1.2 trillion to $14.3 trillion. China's exponential growth has allowed the CCP to invest additional resources into building up a capable, modernized and proficient military, including a world-class navy.

With its frequent forays into Japanese waters, flyovers across the Taiwan Straits, and trillion-dollar Belt and Road initiative in Eurasia, China is doing what rising powers have done throughout history — translating its economic success into geopolitical leverage. A US policy of containment would have the adverse affect of heightening the sense of alarmism in Beijing.

The U.S. can and should compete with China economically. But it should do so responsibly in order to prevent this competitiveness from drifting into military affairs.

A decoupling from China, Washington's largest trading partner outside of North America, is not a realistic proposal. A complete severance of economic ties will produce unprecedented pain for middle-class Americans and roil the international financial system.

A military-to-military showdown, meanwhile, simply entrenches hardline positions in both Washington and Beijing and lessens the credibility of those who call for dialogue and deescalation.

#### China rise is peaceful now---encirclement makes it fast and hostile.

Goldstein 20, associate professor in the Strategic Research Department at the US Naval War College. (Lyle, 7-22-2020, "China’s Putative Threat to U.S. National Security", Published in *A Dangerous World? Threat Perception and U.S. National Security*, https://www.cato.org/publications/publications/chinas-putative-threat-us-national-security)

Factions and interests on both the right and the left are now disturbingly united in an effort to cast China as the next multidimensional threat to the U.S.—on par with or even exceeding that of the Soviet Union in its dimensions. Many of those interests, moreover, are poised to profit from such a characterization. A few obvious facts, however, are worth repeating when considering the putative threat posed by China to U.S. national security: China has not resorted to any significant use of force in more than three decades, it has no foreign bases, and it remains rather weak (compared with U.S. forces) in the domains of power projection and nuclear war fighting. In the coming decades, all of those metrics may reverse, and China could morph from a bungling, paranoid panda into a fire‐​breathing, goose‐​stepping dragon. It seems likely that Beijing will have the requisite resources, bureaucratic discipline, and talent to make such a transition. Moreover, it is not short of strategists advocating for more aggressive steps to counter the United States.41 Washington’s overall goal should be to forestall that metamorphosis, in part by acknowledging China’s security concerns and by seeking compromises on the many issues that divide the United States and China, as outlined in the previous section. It is worth reiterating that Beijing is planning neither to attack the United States nor to conquer East Asia. Rather, its foreign policy behavior has, by and large, comported itself well with current international norms—in rather stark contrast to Moscow’s much more confrontational approach toward the West.

#### US retrenchment prevents war from status competition and gives China a peaceful stake in the current order

**Ward, 17** - Assistant Professor of Government at Cornell University (Steven, Status and the Challenge of Rising Powers, p. 217-218

The former approach is one that few policymakers and scholars openly promote.23 If the United States is interested in avoiding the creation of a deeply revisionist, anti-Western China, it needs to accommodate China’s status claims. Since these likely include the right to a sphere of influence in East Asia, accommodation would likely have to involve a reduction of the American military presence and American influence in that region. This does not mean conceding global leadership to China. Rather, the aim would be to acknowledge that China, as a great power, deserves the same rights that the United States does in world politics – including the right to manage East Asia and the South China Sea the way that the United States manages Latin America and the Caribbean.

This approach carries with it great risks and costs as well.What would be the effect on navigation and trade through the South China Sea? Would important American allies like Japan and South Korea turn into Beijing’s vassals? What if an American withdrawal from East Asia produces a regional arms race? And what if China grows more ambitious rather than more satisfied as the United States withdraws overseas?

But accommodation/retrenchment also has some important advantages. Foremost among them is that it avoids antagonizing Beijing: it is premised upon the idea that, all else equal, accommodation is preferable to denial because denial activates forces that empower hardliners. Accommodation holds out the possibility of empowering moderates and facilitating China’s integration within a reformed version of the liberal international order that has served its economic interests well. Another advantage is that accommodation/ retrenchment is cheaper than any approach involving containment. Retrenchment would reduce American military expenditures while simultaneously creating incentives for other regional powers to bear a greater share of their defense burdens. The United States could return to an offshore balancing posture, which would allow it to redeploy to the region only if China tried to overthrow the new version of the status quo order by, say launching a war in East Asia. But by not signaling status denial, Washington would short circuit one of the major causes of radical revisionist challenges in history, thereby reducing the likelihood that active onshore balancing would be necessary.