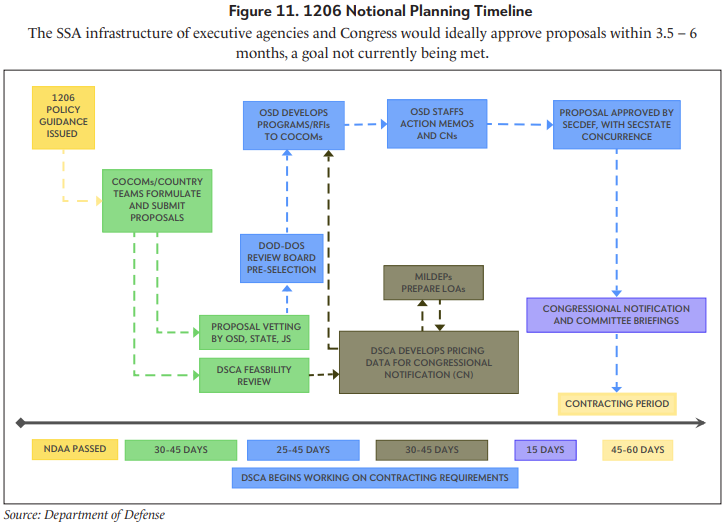
# NEG DA—DoD O/S

### FYI – SC Planners

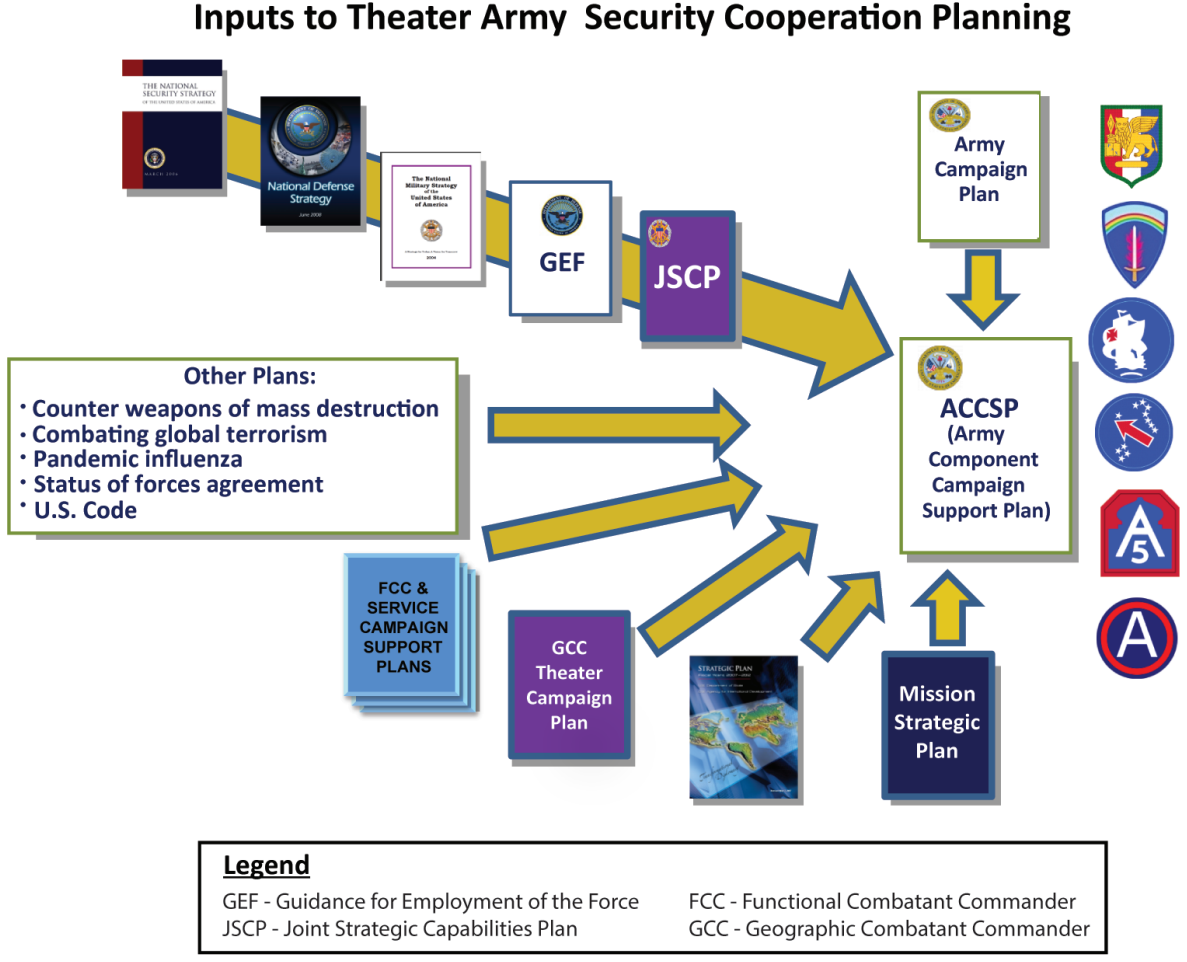
#### What Happens After Fiat

Neptune 16 Neptune, veteran owned and operated strategy and advisory firm, “U.S. Security Cooperation Review,” February 2016, <http://neptuneasc.com/site/wp-content/uploads/2015/05/Neptune-Whole-of-Government-U.S.-Security-Cooperation-Review-20160208.pdf> /GoGreen!



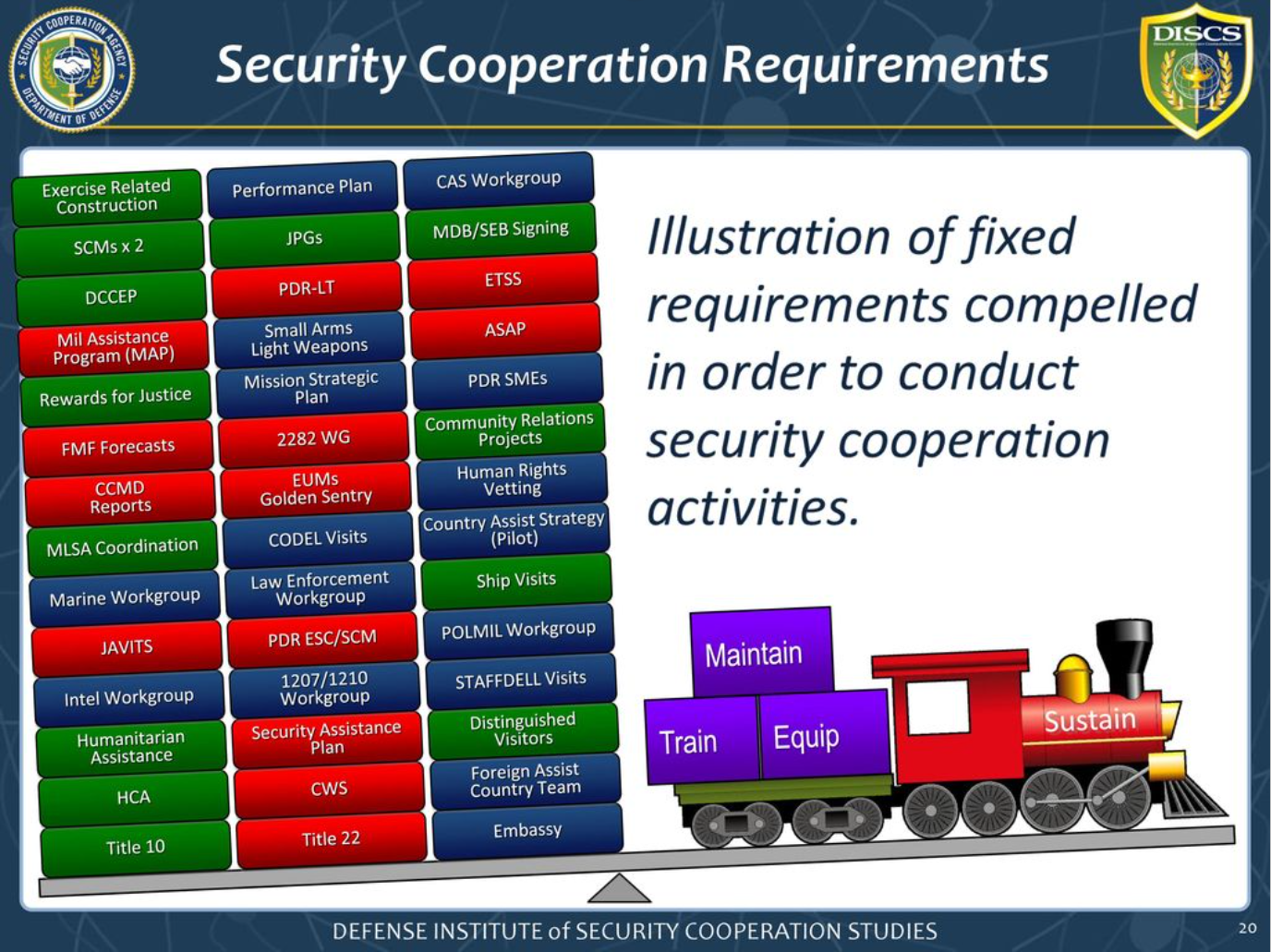
#### Plans Within Plans

Hartmayer 16 Michael S. Hartmayer, Analyst, Center For Army Lessons Learned (CALL), “Security Cooperation: Lessons and Best Practices,” Security Cooperation Bulletin 16-09, March 2016, <https://usacac.army.mil/sites/default/files/publications/16-09.pdf> /GoGreen!



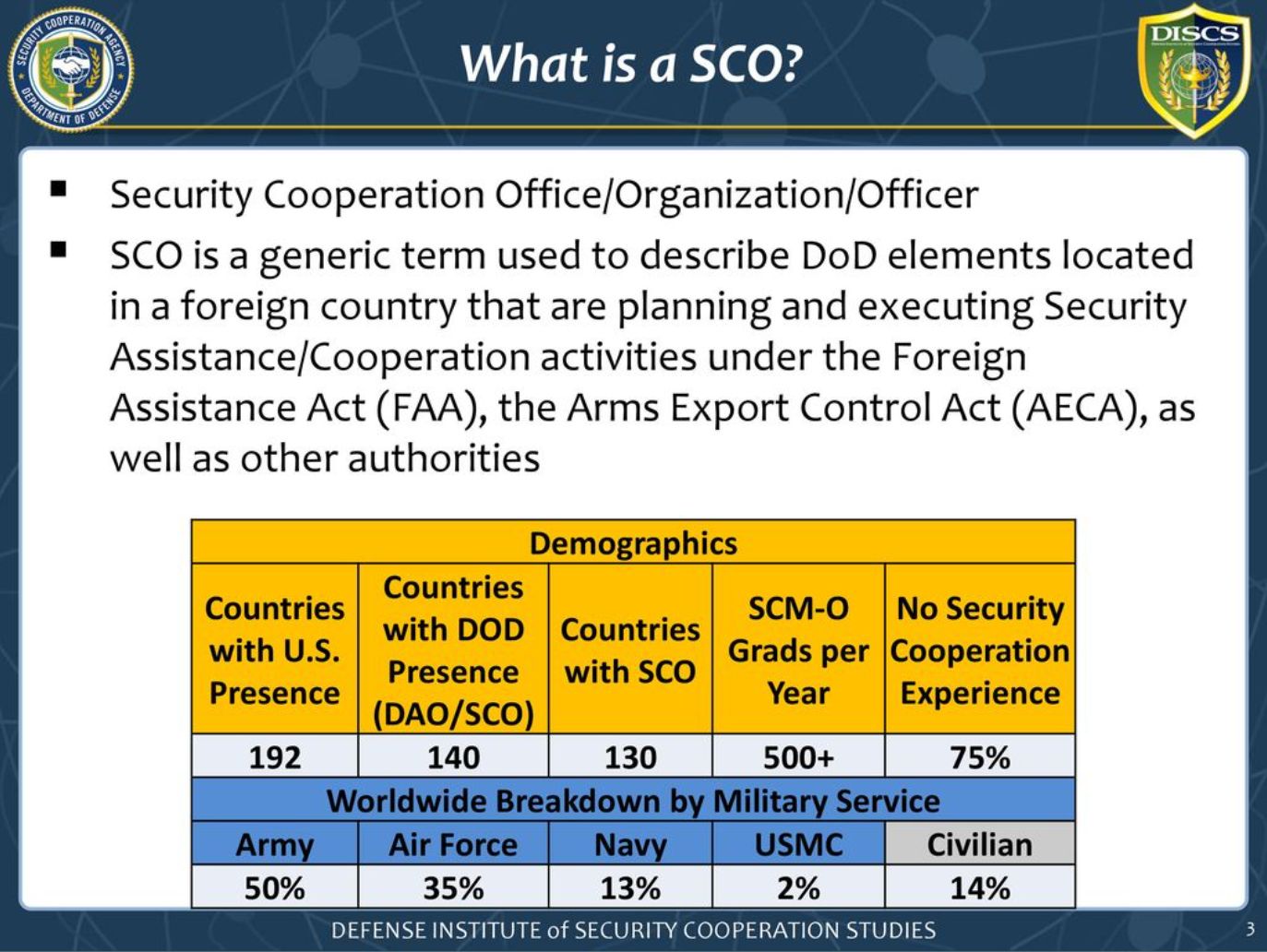
#### Every SC activity has to formally verify compliance with a bevy of required screenings, funding restrictions, and Congressional and interagency reporting requirements, and be scheduled in way that doesn’t disrupt other legally required activities – it’s a lot of paperwork!

DoD 17 Defense Institute of Security Cooperation Studies (DISCS), U.S. Department of Defense, “Security Cooperation Organization (SCO) Responsibilities,” Lesson #0674, 2-21-2017, <https://slideplayer.com/slide/11897298/> /GoGreen!



#### Planners are mostly military personnel on 2-year rotations, hence 75% have “no security cooperation experience”!

DoD 17 Defense Institute of Security Cooperation Studies (DISCS), U.S. Department of Defense, “Security Cooperation Organization (SCO) Responsibilities,” Lesson #0674, 2-21-2017, <https://slideplayer.com/slide/11897298/> /GoGreen!



### FYI – AM&E

#### What AM&E is and why it’s hard

O’Mahony 18 Angela O’Mahony, associate dean for academic affairs at Pardee RAND Graduate School and a senior political scientist at RAND, former assistant professor of international political economy and economic statecraft at the University of British Columbia, PhD political science, UCSD; Ilana Blum, researcher at RAND; Gabriela Armenta, researcher at RAND; Nicholas Burger, senior economist at RAND and director of RAND’s Washington office; Joshua Mendelsohn, researcher at RAND; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Steven W. Popper, researcher at RAND; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; and Thomas S. Szayna, senior political scientist and former director of RAND's Defense and Political Sciences Department at RAND, MA international relations, Claremont Graduate School; “Assessing, Monitoring, and Evaluating Army Security Cooperation: A Framework for Implementation,” RR2165, RAND Corporation, 2018, <https://apps.dtic.mil/sti/pdfs/AD1056354.pdf> /GoGreen!

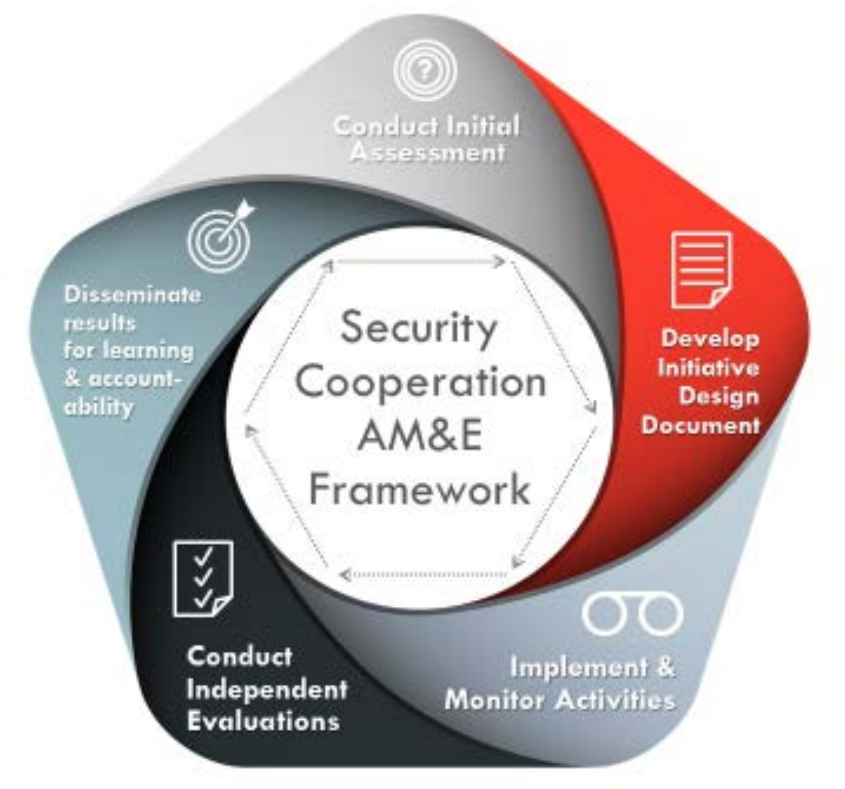
Evaluating the effectiveness of security cooperation in a systematic and rigorous way, however, is challenging, particularly at the Army Service Component Command (ASCC) and Headquarters, Department of the Army (HQDA) levels. First, while security cooperation activities tend to be short term and specific, the strategic theater objectives that security cooperation activities are designed to accomplish are often long term and not well defined. Second, the causal relationships that link security cooperation activities to desired outcomes are often not well understood. Finally, collecting information relevant for evaluating security cooperation effectiveness can be difficult. Although all Army security cooperation activities should be assessed through objective and rigorous after-action reporting and all security cooperation tasks should be evaluated through measures of performance and measures of effectiveness, current Army security cooperation is constrained by poor collection of relevant information.

Regardless of the difficulties inherent in evaluating security cooperation activities, the Army and, more broadly, the Department of Defense (DoD) are facing congressional pressure for increased accountability. In response, the DoD is developing an assessment, monitoring, and evaluation (AM&E) policy for its security cooperation enterprise. In the DoD’s AM&E construct, assessment refers to baseline assessments for leaders and planners that address questions like these: What is the security environment in which these activities will take place? What are the partner’s existing capabilities, and what does the United States want to improve? How well aligned are the partner’s interests and values with those of the United States? Monitoring means tracking efforts to determine whether inputs (e.g., money and effort) are translating into outputs (e.g., equipment, training, education, and information). These outputs then serve as the basis for tracking progress toward objectives (i.e., outcomes). Evaluation examines outcomes and is crucial to understanding what is working and what is not. Success is not ultimately measured by the provision of equipment or training; it is measured by the extent to which security cooperation activities help achieve U.S. objectives. Investments require following up to make sure that they yield the full potential benefits that were expected.1 This study provides a framework and a tool to help the Army improve its

security cooperation AM&E capabilities in line with emerging DoD guidance.

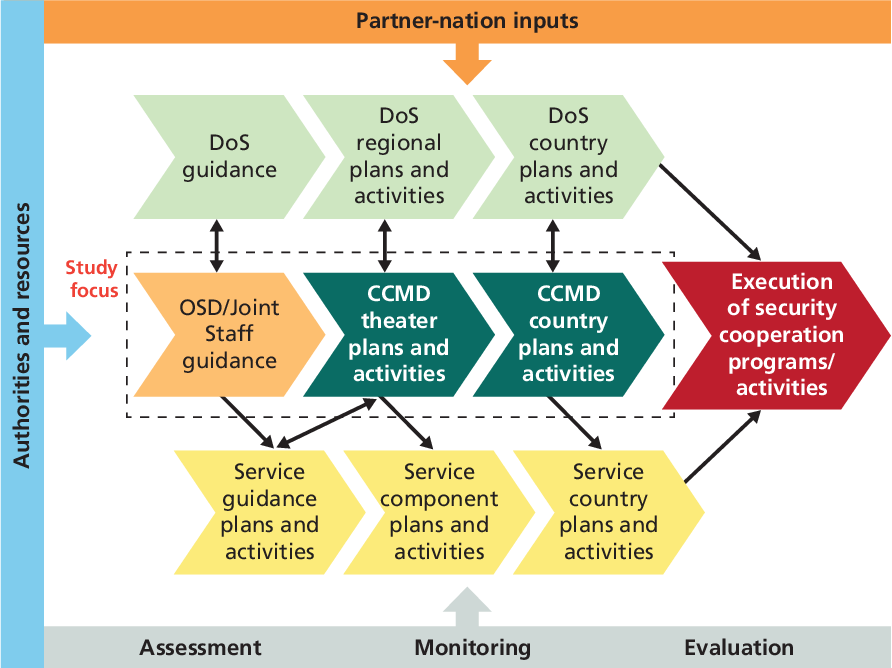
#### It’s an iterative process

DoD 17 Office of the Under Secretary of Defense for Policy, U.S. Department of Defense, “Assessment, Monitoring, and Evaluation Policy For The Security Cooperation Enterprise,” DoDI 5132.14, 1-13-2017, <https://open.defense.gov/portals/23/documents/foreignasst/dodi_513214_on_am&e.pdf> /GoGreen!



#### How AM&E relates to the different civilian and military stakeholders, each with different plans (see “plans within plans” above), involved in SC planning

McNerney 16 Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; S. Rebecca Zimmerman, Policy Researcher at RAND; and Ariel Klein, Naval Strategy and Policy Expert, U.S. Navy, MA Strategic Studies, Air War College, MA Organizational Management, The George Washington University; “SMART Security Cooperation Objectives: Improving DoD Planning and Guidance,” RR-1430-OSD, RAND Corporation, 2016, <https://www.rand.org/pubs/research_reports/RR1430.html> /GoGreen!



## 1NC

### 1NC – DoD O/S DA

#### DoD planners are prioritizing assessment, monitoring and evaluation (AM&E) now

Gould 22 Joe Gould, senior Pentagon reporter for Defense News, “For America’s security aid programs, who will run the show?” Defense News, 4-11-2022, <https://www.defensenews.com/global/the-americas/2022/04/11/for-americas-security-aid-programs-who-will-run-the-show/> /GoGreen!

The Pentagon’s efforts

In an interview with Defense News, the assistant secretary of defense for strategy, plans and capabilities, Mara Karlin, said the Pentagon is already undertaking significant organizational reforms aimed at better coordinating and scrutinizing security assistance programs.

The changes, spearheaded by Undersecretary of Defense for Policy Colin Kahl and executed in December, moved the Defense Security Cooperation Agency ― which manages foreign military sales as well as international military education and training ― under Karlin’s office. What had been the DoD’s security cooperation programs were combined with elements of the Office of Stability and Humanitarian Affairs.

“Hopefully that helps us take a more strategic approach to security cooperation more broadly,” Karlin said several weeks after she and Lewis testified together before the Senate Foreign Relations Committee.

As required by the 2017 defense authorization act, the Pentagon is critically reviewing its own efforts, Karlin said, noting several studies are underway to evaluate whether its security assistance programs were successful.

“The U.S. military, has worked with partner militaries quite robustly since World War II in particular,” she said. “There was a bit of a sea change in the post-9/11 era, and I think that now as we move forward into a different era, we see the urgent need to look at how and in what ways we’re achieving our goals.”

Beyond the 2022 defense policy bill’s mandate for a commission to study U.S. involvement in Afghanistan from 2001 to 2021, the Pentagon is contracting with an outside agency for a comprehensive assessment of the strategic and operational lessons collected from the war there, Karlin said.

It has other efforts afoot to find and disseminate the lessons from its security cooperation efforts.

“We’re developing a learning and evaluation agenda for partnerships that focus on evidence-based policymaking, which will include the most critical learning questions for security cooperation, and prioritize a range of evidence-building activities, including evaluations, monitoring, research studies and tabletop exercises,” Karlin said. “These are hard issues to figure out, and you need to make some kind of a quantitative and qualitative approach.”

For example, the DoD made public a seven-page internal study of U.S. Africa Command’s maritime security cooperation activities in the Gulf of Guinea from 2007 to 2018. It found those efforts managed to spur Ghana and Senegal to an increased interest in policing their waters. But on the flip side, maintenance and parts issues plagued the effort, which included riverine patrols and offshore interdiction of illegal fishing and human trafficking.

#### Plan overstretches them

Thaler 16 David E. Thaler, Senior International/Defense Researcher at RAND, MIA International Security Policy/Middle East, Columbia University; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Beth Grill, Senior Policy Analyst at RAND, MA Middle Eastern Studies and Economics, Johns Hopkins University School of Advanced International Studies; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; and Amanda Kadlec, RAND; “From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation,” RR1438, RAND Corporation, 2016, https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1400/RR1438/RAND\_RR1438.pdf /GoGreen!

The proliferation of complicated authorities has led to a number of pernicious effects in DoD’s SC enterprise. Two deserve mention here. First, authorities and related programs require that staff in DoD stakeholder organizations—particularly the CCMDs, OSD, and the agencies—are available to plan their use and develop initiatives or events, shepherd them through the myriad justification and approval processes, and manage and report on their execution. The greater the number of authorities required to achieve stakeholder objectives, the larger the staff required to properly manage them. But at the same time, the catalog of authorities has expanded, while budget cuts have required staff contraction across DoD. This leaves stakeholders with “too many programs…and not enough people to execute” because “we are losing people who manage the programs.”28 While OSD has at times sought to hone a reach-back capacity to provide advice to the CCMDs, the expanding catalog of authorities still requires a larger staff to properly manage them. This forces SC personnel to consider the cost-benefit of doing some events with multiple funding sources given the man-hours and workload required to manage use of separate authorities, whereby “small programs aren’t worth the time.”29 This also leads to programs that are not executable in the field.30

#### Empirically halts progress on AM&E – key to effective strategic competition

Shah 18 Hijab Shah, research associate with the International Security Program at the Center for Strategic and International Studies (CSIS); and Melissa Dalton, senior fellow and deputy director of the CSIS International Security Program; “Security Cooperation as a National Defense Strategy Tool,” Commentary, Center for Strategy and International Studies, 10-3-2018, <https://www.csis.org/analysis/security-cooperation-national-defense-strategy-tool> /GoGreen!

Ensuring Return on Investment

Pooling resources and sharing responsibility with partner forces is a critical aspect of U.S. efforts to best strategic competitors as described within the NDS. However, despite billions of dollars’ worth of grant-based security assistance to its allies and partners—with another $3.4 billion approved for FY 2019—the United States has yet to see the proportionate returns from its investment in foreign countries’ security capabilities. In several areas, U.S. partners are not yet ready to shoulder the burdens that the U.S. administration seeks of them with gaps in professionalization, modernization, and interoperability with U.S. forces. Growing assessment, monitoring, and evaluation (AM&E) standards and mechanisms to enable the U.S. government to track how its investments are being utilized and to what extent shared U.S. and partner goals are being achieved, as mandated by the FY 2017 and 2018 National Defense Authorization Acts, will help. However, the lack of high-level policy prioritization for these tasks, exacerbated by staff capacity and workforce shortfalls, have resulted in some useful steps forward but slow progress overall.

The U.S. government should consider approaching security cooperation from a return-on-investment lens, articulating and implementing clear and practical AM&E standards, benchmarks, corrective measures, and results in support of strategic objectives. Better AM&E could pave the way for a greater return on investment and therefore result in reliable, capable partnerships that provide the United States an edge over its strategic competitors.

Conclusion

Security cooperation is not a strategy unto itself but is clearly a critical way to achieve strategic aims. The U.S. government should pursue security cooperation with a clear-eyed assessment of the risks and tradeoffs for the sake of “improving a relationship,” weighed against operational, economic, and humanitarian considerations. With growing impulses to burden-shift global security requirements onto allies and partners, the United States will have to resist temptations to rush into security cooperation commitments. It will have to build policy frameworks and technical approaches that are both rigorous and responsive to enable it to compete and secure its objectives in the twenty-first century.

#### Failure is existential – integrated deterrence is key – NOT any one tech

Shaw 21 Ryan Shaw, Senior Advisor and Professor of Practice in History and Strategy at Arizona State University, PhD, MA history, Yale University, BA American Government and Politics, US Military Academy at West Point, “In Defense of Competition,” Real Clear Defense, 11-11-2021, <https://www.realcleardefense.com/articles/2021/11/11/in_defense_of_competition_803143.html> /GoGreen!

As the Pentagon readies its new National Defense Strategy, the commentariat—unsurprisingly—has some thoughts. While the perspectives are, no doubt, as varied as the array of think tanks and universities from which they spring, there seems to be a significant piling on against both the “Great Power Competition” that animated Trump-era guidance and the (allegedly distinct) “Strategic Competition” terminology advanced by the Biden administration. But “competition” is a rare instance of bipartisan continuity because it speaks to real and important dynamics in the international system, and it has led to important new thinking in our approach to national security. We should not be so quick to discard it.

Rather than abandoning competition, it is time now to double down. The Pentagon strategy should embrace a robust concept of integrated deterrence, and the White House should lead with a National Security Strategy (NSS) rooted in a holistic approach to Competitive Statecraft.

The critics are right that Great Power Competition (“GPC”) has become a vacuous catch-all, a magic word, as CNAS’s Wasser and Pettyjohn tell it, that can justify “every force, capability, or resource request.” But that’s a perennial bureaucratic tendency; the same was true of CT and then COIN in the Bush and Obama years, and probably any number of terms du jour in prior eras. We should always work to minimize these abuses, but we won't eliminate them as long as we use words to describe our priorities. Other critiques are less valid and far less helpful.

The idea that an emphasis on competition precludes the possibility of cooperation is an unhelpful reductio ad absurdum. Pundits may not be able to sustain two competing ideas at once, but the international system always does, and the military clearly can: emerging U.S. doctrine envisions a competition continuum, in which “the joint force… campaigns through a mixture of cooperation, competition below armed conflict, and armed conflict calculated to achieve the desired strategic objectives.” As Daniel H. Nexon points out, “Even during the Cold War, the United States and the Soviet Union worked out a variety of formal and informal rules that helped them manage competition, limit nuclear proliferation, and otherwise structure international relations.” (It is unclear how Nexon intends this observation to support his argument against competition.)

Equally unhelpful is the common complaint that the phrase “‘strategic competition’ reflects uncertainty about what that competition is over and what it means to win.” Here again, while it might stymie the pundits, this intellectual hurdle seems not to have tripped up our military leaders—they have been consistent in identifying the stakes of this competition as the “rules-based international order that brought prosperity and relative peace for the last seven decades.”

And “what it means to win” is just the wrong question—that’s the whole point. Echoing George Kennan ("We have been handicapped … by a popular attachment to the concept of a basic difference between peace and war…"), the competition discussion is enabling the military to finally—against all odds—shed the idea of war as a finite game that starts with an opening salvo of munitions and ends with a ceasefire and a treaty. The fixation on “winning” breeds fatal short-termism—see the common refrain that we didn't fight a twenty-year war in Afghanistan, but rather twenty one-year wars.

What all these simplistic critiques miss is the simple old truth that the enemy gets a vote. Nexon wants us to consider competition as a means rather than an end. But it’s neither—it’s just a plain fact of our strategic environment, and the last round of guidance intended to highlight it as the most salient one for U.S. strategy. It may or may not have been true, but we operated for much of the last thirty years as though we did not have any real competitors, ideologically or materially. The “end of history” trope after the Cold War was premised on the absence of an ideological alternative to liberal democracy; and if 9-11 proved that wrong, the “asymmetric” modifier we appended to the “warfare” of the Global War on Terror reassured us that proponents of radical Islam lacked the resources to make their vision an existential threat.

But the long-term ascendency of liberal, democratic ideals and rules-based international order is neither inevitable nor irreversible. There are alternatives on offer, and they are actively being pursued by adversaries whose capabilities across many domains threaten to eclipse our own in the not-so-distant future. These are the facts, and they demand our attention. The last NSS and NDS were right to frame them that way.

We must prevent the loss of our competitive advantage and deterrent capacity in conventional and nuclear warfare—competition should not prevent that; properly conceived, competition demands it. (The Pentagon understands this, too.) But the most pernicious element of these arguments against competition is the insinuation—or the outright assertion—that we can or should focus on high-end capabilities to the exclusion of all else. This requires a willful disregard of everything we have learned about the gray zone/hybrid warfare/choose-your-appellation. After all, while our high-end advantage has eroded, it is not gone. We have so far deterred major conventional and nuclear war, but our adversaries—especially those near-peer “great powers”—have found countless ways to improve their strategic position and degrade ours without triggering a conventional military response. High-end deterrence is necessary, but it’s clearly not sufficient. The accumulation of minor setbacks can be existential, not just because of their obvious and immediate effects, but because they can degrade our long-term ability to generate and project conventional power.

For all its emphasis on GPC, the last NDS recognized the interrelated nature of threats at all points on the competition continuum. This was made especially clear in the Irregular Warfare Annex: “State adversaries and their proxies increasingly seek to prevail through their own use of irregular warfare, [suggesting] the need for a revised understanding of IW to account for its role as a component of great power competition.”

What we need is not a narrower concept of deterrence but a broader one that focuses not just on the future conflict we could lose but also on the ongoing competition we are currently losing. Perhaps this is where Secretary Austin’s nascent “integrated deterrence” idea is headed. He seems to want to integrate across domains and technologies and with allies, and who could argue? Well, lots of people, including Representative Mike Gallagher (R, WI), who has apparently been reading his Pettyjohn: “What we actually need to integrate is more conventional hard power—more ships, more long-range missiles and more long-range bombers in the Indo-Pacific.”

Gallagher here is giving voice to a perpetual false choice we frame between conventional and irregular capabilities. But as the IW Annex said, competing in the contested space “does not require significant new resources… it requires new ideas and new means of employing existing capabilities.” The limiting factor is not in our pocketbooks, it’s between our ears. Educating for IW may not lead to great photo-ops, but it could lead to better outcomes below the threshold of major war, which would be worth a great deal more. Unfortunately, after our inglorious exit from Afghanistan, it seems we are determined to repeat what the Annex called “the ‘boom and bust’ cycle that has left the United States underprepared for irregular warfare in both Great Power Competition and conflict.”

Some Congressional leaders are pushing back. Last year's NDAA included authorization to establish a DOD center for studying irregular warfare. This year's bill is still in draft, but both chambers have provisions demanding an implementation plan for the IW Annex, and the House bill would require a report on the establishment of the center. Educating for IW may not lead to great photo-ops, but it could lead to better outcomes below the threshold of major war, which would be worth a great deal more.

With all due respect to Secretary Austin, an integrated deterrence worth its name would be integrated both vertically and horizontally. Vertically, it would supplement our nuclear and conventional deterrence with unconventional deterrence to provide creative and seamless response options other than “do nothing” and “all-out war.” Horizontally, along with allies and partners, it would integrate military force with the other instruments of U.S. national power.

## !—GENERAL

### ! O/V

#### Effective SC-driven partnerships are independently key to prevent escalation to extinction from BOTH abandonment AND entanglement risks

Frühling 21 Stephan Frühling, Associate Dean, Partnerships and Engagement in the College of Asia and the Pacific at The Australian National University, former ‘Partner across the Globe’ research fellow in the research division of the NATO Defense College; and Andrew O’Neil, Acting Dean of the Graduate Research School and Professor of Political Science at Griffith University, formerly worked with Australia’s Department of Defence; “Alliances, Nuclear Weapons and Escalation,” Chapter 1, *Alliances, Nuclear Weapons and Escalation: Managing Deterrence in the 21st Century*, eds. Frühling & O’Neil, ANU Press, 2021, ISBN 9781760464912, pp.1-5 /GoGreen!

As great power competition once again assumes a central place in international relations, alliances have taken on renewed importance in the security calculations of Australia and other US allies in the Indo-Pacific and Europe. Deterrence of an attack on allies is a core function of US alliances, as are mechanisms through which states seek to manage the risk of escalation—the movement through increasing intensity of conflict up to, in the extreme, global nuclear war.1 Alliances seek to prevent escalation in the form of an attack on its members through strategies of deterrence and extended deterrence that are themselves predicated on credible threats of escalation. Nuclear weapons are central to deterrence and escalation considerations and form a key component of America’s strategic toolkit to reassure Japan, South Korea and Australia in the Indo-Pacific, as well as North Atlantic Treaty Organization (NATO) allies in the Euro-Atlantic.

However, allies cannot afford to be passive actors in their interactions with Washington. They need to prepare for and seek to manage escalation in a broader geostrategic, technological and political context that shapes the ability of alliances to adapt to a new security environment. While the challenge of great power competition is acute at both ends of Eurasia, adversary threats, geography and the institutional context of US alliances differ. This volume brings together contributors from Europe, North-East Asia, the United States and Australia to better understand these challenges, identify commonalities and differences across regions, and pinpoint ways to collectively manage nuclear deterrence in twenty-first century alliances. It focuses on nuclear deterrence in the Indo-Pacific and strategic competition between the US and China; the role of non-nuclear US allies in the Indo-Pacific and Europe in supporting US extended nuclear deterrence; political-military challenges in alliance plans for escalation; allied perspectives on the consequences of new non-nuclear capabilities, including cyber and hypersonic weapons, for deterrence and strategic stability; and lessons on how the US and allied nations can better engage their respective publics on questions relating to nuclear deterrence.

Alliances, Escalation and Nuclear Weapons

How to manage escalation is an inherently political question. The costs and benefits of support in case of attack and of achieving security against specific challenges will differ between allies. The credibility of extended deterrence threats rests on the commitment of certain allies, especially the US, to provide security to other allies who find themselves under more immediate threat. The asymmetric nature of an extended deterrence relationship thus creates anxieties of abandonment on the part of the threatened ally and fears of entrapment by all allies in conflicts in which they have little direct stake. For deterrence to be effective, allies nonetheless have to find ways to agree and credibly commit to what they are willing to do for each other.

Nowhere is this more important than in relation to the role of US nuclear weapons in America’s alliances. While some US allies have previously expressed sympathy for the Treaty on the Prohibition of Nuclear Weapons (TPNW), none today is willing to sign it, as their focus has turned to the challenge of managing escalation in potential great power conflicts in Europe and the Indo-Pacific. Moscow’s penchant for nuclear sabre-rattling in crises with NATO and Ukraine, Beijing’s ambitious nuclear force modernisation, North Korea’s development of a thermonuclear and intercontinental range arsenal, and the development of new capabilities— including hypersonic missiles designed to confer escalation advantage over the US and its allies in regional conflicts—have all roused nuclear strategy from its post–Cold War hibernation. From 2011, the Obama administration established extended deterrence dialogues with North-East Asian treaty allies, Japan and South Korea, in response to growing concerns about North Korea and China. Since 2014, the NATO alliance has paid far greater institutional and political attention to the strategic role of its nuclear forces, and to the possibilities of escalation more generally after the end of the Intermediate-Range Nuclear Forces (INF) Treaty. Under the Trump administration, US nuclear policy was notable for how little controversy it attracted among US allies, despite the administration’s decision to introduce the first new (low-yield) warhead variants since the end of the Cold War.

However, the existential dependence of US allies on decisions taken in Washington about US nuclear strategy has been a constant element in the history of US alliances, and key to grasping their inherent tensions: from US Secretary of Defense Robert McNamara’s challenge to NATO’s nuclear strategy of massive retaliation in the early 1960s, to concerns about US– Soviet arms control undermining the security of Western Europe in the 1970s and the late 1980s, to President Obama’s declared commitment to reducing the role of nuclear weapons in US defence posture in the face of rising nuclear threats to North-East Asian allies. Throughout the Cold War, arguments about nuclear strategy were staple fare for official and academic debates, especially regarding the role of nuclear weapons in deterrence. How to interpret and implement the concept of flexible response after its adoption in 1967 was the subject of often acrimonious debate in NATO, as allies sought to balance fears of abandonment, entrapment and a Soviet Union that threatened them all, but in different ways depending on their geographical position. In Asia, forward-based US nuclear forces on the Korean Peninsula were a central element in deterring North Korea until their withdrawal in 1992, and Japan carefully balanced its public aversion to nuclear weapons with practical support for the operation of US nuclear forces as a deterrent against the Soviet Union and China. In Australia, the role of the ‘joint facilities’ in US nuclear operations was a central element of the alliance in the second half of the Cold War.

Managing Escalation in the Indo-Pacific and Euro-Atlantic Areas

At the 2021 Munich Security Conference, President Biden declared that ‘America is back’, and that ‘the United States is determined … to earn back our position of trusted leadership’.2 However, while it is clear that public division and disagreement among allies about how to manage escalation and deter threats are undesirable, the US and its allies still have a long way to go in either the Indo-Pacific or the Euro-Atlantic areas to develop viable and commonly accepted political-military strategies for the new era of great power competition.3 Significant differences remain between the challenges of escalation at either end of Eurasia, but the basic problem— how US allies can achieve political agreement on credible threats of military escalation, including through the use of nuclear weapons, to deter attacks by nuclear-armed powers—remains the same. Hence, the value of exchanging ideas between the Indo-Pacific and Euro-Atlantic areas is also far greater than it has been in the past.

In the 1980s, a US official reportedly observed that exchanges between NATO and Japan throughout the INF negotiations had ‘taught the Japanese to speak German’.4 The Reagan administration’s decision to abrogate US obligations towards ANZUS (Australia, New Zealand, United States Security Treaty) ally New Zealand was also in large part motivated by sending signals to Washington’s Scandinavian allies, some of whom at the time were flirting with anti-nuclear initiatives.5 However, the institutional and geostrategic context of US alliances in Europe and the Asia-Pacific was sharply different during the Cold War, as was their manner of engagement on questions of escalation and nuclear strategy. Today, these differences are far less pronounced, and the US, its Indo-Pacific allies and NATO are rediscovering the political-military challenges of escalation management at the same time. In the context of China’s rise, North Korea’s nuclear tests and the US retirement of its nuclear-armed, submarine-launched cruise missiles in the 2010 Nuclear Posture Review, Japan and South Korea pressed US officials for ‘more NATO-like’ extended deterrence arrangements.6 NATO allies, for their part, increasingly recognise the relevance for their alliance of a possible conflict with China.7 For several years, NATO’s institutional architecture has been explicitly drawn on by Japanese security analysts to support proposals to strengthen nuclear deterrence and reassurance in the US–Japan alliance.8 Even in Australia, former prime minister Kevin Rudd—whose government in 2008 co-sponsored the Australian–Japanese International Commission on Nuclear Non-Proliferation and Disarmament—joined calls in 2021 for an ‘Asian Nuclear Planning Group’ that would allow the US, Australia, Japan and South Korea ‘to discuss specific policies associated with US nuclear forces and conduct war games and exercises, including those involving the highest political-level participation’.9

### T/C – GPC Turns I/Ls

#### Turns case – even absent great power war, failing competition makes their advantage impacts more likely

Clare 22 Stephen Clare, Research Fellow at the Forethought Foundation for Global Priorities Research, MSc Renewable Resources, McGill University's Department of Natural Resource Sciences, BA, BS, Sustainability Studies, McMaster University, “Modelling Great Power conflict as an existential risk factor,” Effective Altruism Forum, 2-3-2022, <https://forum.effectivealtruism.org/posts/mBM4y2CjfYef4DGcd/modelling-great-power-conflict-as-an-existential-risk-factor#III__Category_1__International_tension> /GoGreen!

First, I want to show how tensions between Great Powers can affect existential risk even if they don’t lead to direct conflict.

The history of nuclear risk demonstrates this effect. Nuclear weapons are arguably the greatest threat to the long-term future that humanity has created so far. While they were invented during World War II, their proliferation and the invention of new delivery mechanisms such as submarines and intercontinental ballistic missiles occurred after the war, amid mutual fear of conflict between the US and Soviet Union.

By international tension I mean something like “a shared worry about an imminent conflict [which] itself may contribute to starting a war”.[13][14] There’s at least two specific dynamics worth worrying about if international tension is high in the 21st century.

The first is that hostilities will probably make it harder for countries to coordinate to mitigate other risks. As a recent example, progress towards a strong, international treaty governing lethal autonomous weapons was reportedly stymied by the US and Russia. We might expect the effect on risks like future pandemics, governance of new technologies, or climate change to be similarly negative. However, I’m very uncertain about the size of this effect. In some ways a more divided world may be even more resilient to certain risks if it helps avoid correlated policy failures. The Covid-19 pandemic could have been even worse, for example, if every country had a policy that was similar to those adopted in a country like the US.

The second dynamic is that international tension could speed up the development of dangerous technologies like military AI, new weapons of mass destruction, and other weapons that are hard to foresee in 2022. Militaristic competition is particularly intense, paranoid, and aggressive. The more likely they think a war is, the more likely decision-makers are to make large and risky investments in military technologies to try to gain an advantage over their rivals.[15] Once these weapons are developed, they could be deployed unintentionally, as nearly occurred with nuclear weapons on several occasions during the Cold War.

Again, though, I’m uncertain about the size of the effect. I also think there is some upside risk. It seems like states will also be more likely to develop defensive technologies if international tension is high. These defenses could be helpful in mitigating accidents as well as purposeful attacks. So if the probability that an accident is avoided outweighs the probability that an attack is successful, a more tense world could be a safer one.

For these reasons, I think Great Power relations affect existential risk even if they do not lead to direct conflict. More international tension will increase existential risk to the extent that (1) international tension makes it harder for countries to cooperate and (2) more cooperation reduces risk. The more likely Great Powers think a war is, the more they will increase their military budgets and invest in developing new weapon technologies. But international tension could also decrease risk. For example, it could increase policy diversity among countries which could boost resilience. It could also speed up the development of defensive technologies. I’m very uncertain about the net effect of these dynamics. I think it would be really helpful to see more research in this area.

### T/C – AM&E Turns Solvency

#### Turns solvency – emerging tech SC efforts will be irrelevant or counterproductive without AM&E

Van Eerden 20 Captain James R. R. Van Eerden, deputy director, chief operations officer, and Marine detachment officer-in-charge, National Security Agency, graduate of the Expeditionary Warfare School, Marine Corps University, “Seeking Alpha in the Security Cooperation Enterprise: A New Approach to Assessments and Evaluations,” Journal of Advanced Military Studies, 11(1), Spring 2020, DOI 10.21140/mcuj.2020110105, pp.113-126 /GoGreen!

Abstract: Despite the billions of dollars invested in the security cooperation enterprise each year, the Marine Corps and the Department of Defense (DOD) have failed to implement standardized metrics and processes for evaluating security cooperation engagements at the tactical level. Without such data, it is nearly impossible for the security cooperation enterprise to accurately assess progress in achieving national security objectives, such as partner nation basing access and partner force capacity building. Without clear signposts of progress, cooperation engagements will continue to be hampered by redundant or irrelevant training that limits the return on investment for the DOD and strategic U.S. partners.

Keywords: security cooperation, Marine Corps, Department of Defense, cooperation agreements, national security objectives, return on investment, data, metrics

In the realm of investment banking and equity markets, the term alpha is used to describe financial performance relative to standard market returns during a given period of time.1 For investors, the process of “seeking alpha” requires discipline and careful attention to data and analytics patterns that can ultimately lead to a greater return on investment. Similarly, individuals responsible for managing defense spending should seek to implement standard methodologies and data-based decision-making processes, particularly in high investment areas like security cooperation. At times, the focus on new technological developments, such as artificial intelligence and 3D printing, has distracted from the human dimension of conflict and the “key role in building partner capacity” described in the Marine Corps Operating Concept. 2 While it is vital to continue developing disruptive technology for future warfare, it is equally important to pursue innovation through improvement of existing technology and processes.

Based on numbers provided by the Office of the Secretary of Defense for fiscal year 2019, security cooperation activity accounts for at least $10 billion in spending—a conservative estimate that does not include classified programs or drug-interdiction programs authorized under Section 127e and Section 284c of Title 10 of the U.S.C.3 Each year, the Department of Defense (DOD) conducts 3,000–4,000 security cooperation engagements with more than 130 countries.4 Despite the large investment of money and time in the security cooperation enterprise, the DOD has failed to implement a standard methodology for evaluating security cooperation activity at a tactical level. In light of this, the Marine Corps should implement a standardized, quantifiable, tactical level security cooperation assessment methodology to accurately measure the effectiveness of engagements with partner forces.

Security Cooperation Defined

Security Cooperation, Joint Publication (JP) 3-20, provides the following definition of security cooperation:

Security cooperation (SC) encompasses all Department of Defense (DOD) interactions, programs, and activities with foreign security forces (FSF) and their institutions to build relationships that help promote U.S. interests; enable partner nations (PNs) to provide the U.S. access to territory, infrastructure, information, and resources; and/or to build and apply their capacity and capabilities consistent with U.S. defense objectives.5

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-tomilitary engagements, where the U.S. military engages in training partner forces under the auspices of Title 10 and Title 22 authorities.

The important role of security cooperation in the future operating environment cannot be overstated. The Summary of the 2018 National Defense Strategy of the United States of America asserts that enduring military success is contingent upon “building long-term security partnerships” and upholding “our allies’ own webs of security relationships.”8 In the current operating environment marked by great power competition, security cooperation will be a vital tool used to preempt high-end conflict and assure strategic access to basing, equipment, and intelligence resources. In short, security cooperation is an indispensable pillar of U.S. foreign policy, with the capability to influence all instruments of national power.

Overview of Doctrine and Policies

Though there is much current debate about cost-sharing measures between the United States and its allies, few national security experts would object to the importance of security cooperation. However, it is often difficult to articulate the metrics that define mission success. Perhaps the problem is best framed with a question: If indeed security cooperation is important, how does one measure the output from such activity to shape future planning and funding? This question is only partially answered by doctrine and directives at the joint and Service component levels.

Security Cooperation recommends that all combatant commanders should use an assessment, monitoring, and evaluation framework. However, the publication mistakenly identifies strategic-level assessments and evaluations as the only deficiency in security cooperation planning: “Because SC activities are dispersed and generally support long-term objectives, the impacts can be difficult to immediately measure above the tactical and operational levels (i.e., operational assessments and service or functional component-level evaluations).”9 In January 2017, the Office of the Undersecretary of Defense for Policy published DOD Instruction 5132.14: Assessment, Monitoring, and Evaluation Policy for the Security Cooperation Enterprise, which further elaborates on the assessment, monitoring, and evaluation (AM&E) framework. The DOD instruction outlines the responsibilities of all relevant parties at the strategic level, including the Chairman of the Joint Chiefs of Staff, the geographic combatant commanders, and the functional combatant commanders. The instruction letter states that the “DoD will maintain a hybrid approach to management of AM&E efforts, whereby, in general, assessment and monitoring will be a decentralized effort based on the principles and guidelines established in this instruction and other directives, policies, and law.”10 In theory, this decentralized approach to assessments is preferable. The reality, however, is that Service components have failed to support the Office of the Secretary of Defense’s AM&E framework with focused data inputs.

While the Marine Corps has successfully implemented operational assessments through the use of security cooperation engagement plans and capabilities-based assessments, it lacks the necessary tactical assessments to contribute to the higher-level AM&E structure. In general, the Marine Corps supports the implementation of assessments for security cooperation engagements. Marine Corps Order 5710.6C, Marine Corps Security Cooperation, which governs the conduct of security cooperation activity, suggests that integrated assessment teams are vital to an effective long-term strategy. The order also states that the purpose of assessments is to “provide maximum effectiveness.”11 In addition to the Marine Corps order on security cooperation, Marine Corps Operations, Marine Corps Doctrinal Publication 1-0, affirms the value of assessments. According to Marine Corps Operations, assessments not only provide a “basis for adaptation,” but they also serve as a “catalyst for decision-making.”12 Based on this information, it would seem that the Marine Corps and the joint force have properly identified the need for security cooperation assessments, which prompts the question: What, if anything, needs to be changed about the current approach to security cooperation engagements?

Research Hypothesis

As a former theater security cooperation (TSC) coordinator for Special-Purpose Marine Air-Ground Task Force Crisis Response-Africa 17.1 (SPMAGTF-CRAF 17.1), the author was not aware of any method to accurately measure the performance and effectiveness of security cooperation missions. After reviewing the after action reports submitted by previous teams, there was a noticeable scarcity of specific training data; higher headquarters and the Marine Corps Security Cooperation Group had not promulgated a standardized, quantifiable, tactical-level assessment methodology. Although the author’s personal experiences indicate that security cooperation assessments lacked analytical rigor, additional independent research was used to validate the hypothesis that the Marine Corps lacked a standardized, quantifiable process for evaluating security cooperation missions at the tactical level.

Research Process

The research consisted of two parts: first, the author thoroughly reviewed the seminal doctrinal publications, directives, and policies relevant to the field of security cooperation to determine if an assessment methodology existed. This process entailed a complete review of 16 authoritative documents and articles. Second, the author completed a data-mining project to evaluate after action reports submitted to the Marine Corps Center for Lessons Learned (MCCLL). The data mining spanned six years of SPMAGTF-CR-AF data between 2010 and 2016, excluding 2011. The author’s research included both unit after ac- tion reports and MCCLL reports for security cooperation missions. The source content for the second part of the research project consisted of 19 after action reports, totaling 280 pages of material.

Summary of Findings

The first part of the research project involving the 16 authoritative source documents yielded no additional information about quantitative assessment methodologies. The second part of the research project yielded more instructive results:

• 32 percent of the documents did not provide a single reference to the words “assessment” or “evaluation”

• 68 percent of the documents mentioned the word “assessment” or “evaluation” at least once

• 38 percent of the documents that used the words “assessment” or “evaluation” used them in the context of developing a training schedule or assisting partner nation forces

• 20 percent of the documents explicitly mentioned using training and readiness standards as a baseline for evaluating partner nation forces

• None of the after action reports incorporated quantifiable data or a standard process for evaluating partner force performance and capability

The most salient conclusion from this data is that security cooperation leaders recognize the importance of assessments and evaluations in achieving successful outcomes with partner forces. However, the research also implies that security cooperation leaders have not fully incorporated quantifiable standards into the evaluation process, as evidenced by the lack of data and inconsistent assessment methodologies.

Research Conclusions

Despite the myriad references to assessments and evaluations in doctrine, policies, and mission after action reports, the analysis confirmed that the Marine Corps had not published or even developed a standardized, quantifiable, tacticallevel assessment methodology for security cooperation engagements. Currently, the only feedback received by operational planners is subjective observations from team leaders and team chiefs in the form of after action reports. Marine Forces Europe and Africa (MFEA) headquarters provides limited guidance for developing the after action reports and quantitative data is not required. Most of the reports are replete with anecdotal information, where teams bemoan their lodging conditions or food options, rather than provide specific, action- able data to inform future engagements and planning. This void in the feedback loop means that operational and strategic planners are left without the details necessary to complete their respective higher-level assessments.

A Proposed Solution: Hybrid Training and Readiness Assessment Methodology

Galileo Galilei noted that one should always seek to “measure what is measurable, and make measurable what is not so.”13 Based on the previously mentioned research findings, the security cooperation enterprise has not succeeded in making security cooperation activities measurable at the tactical level. In light of this, the Marine Corps should adopt a hybrid training and readiness assessment methodology for future security cooperation engagements. The joint force should replicate this methodology to synchronize assessment efforts across the DOD.

The Hybrid Training and Readiness Assessment Methodology (hereafter referred to as the “methodology”) was developed and implemented by the author during a SPMAGTF-CR-AF deployment in 2017 and was used during subsequent SPMAGTF-CR-AF deployments. The methodology was lauded by the SPMAGTF-CR-AF commander and reviewed by the Commandant of the Marine Corps in 2017. Senior staff members from the Center for Army Lessons Learned have requested to highlight the methodology as a recommended model for future partner engagements across the Department of the Army.

The methodology is a three-part process consisting of nine individual steps (figure 1). The three parts are planning, execution, and transition, which reflect the various stages of a security cooperation mission. Part one, planning, begins with the security cooperation team leaders and team chiefs completing steps one through three, which consist of mission analysis, T&R selection, and period of instruction development. Part two, execution, encompasses steps four through six that require an initial assessment, a period of instruction, and a final assessment. Part three, transition, includes steps seven through nine, which require TSC teams to compile data from their assessments, analyze the data, and then disseminate conclusions from the data. The outputs from part three feed back into part one as new inputs prior to reinitiating the mission analysis process. Each step of the methodology consists of several questions that should be answered before proceeding to the next step. This nine-step iterative process can be adjusted and tailored to meet the unique demands of each mission.

During part 1, the team leaders and team chiefs are dependent on the embassy country team and MFEA regional planners to relay the specific training requests of the host nation. Operational and tactical level staff must work together to compare Marine Corps T&R standards with the partner nation training requirements. By using Marine Corps T&R standards as a baseline **[FIGURE 1 OMITTED]** and adjusting the standards to meet the partner nation objectives, the security cooperation team employs a hybrid T&R approach, which is used over time to gauge the progress of the partner nation. During part 2, security cooperation team leaders will select one of three different assessment packages to perform the initial and final assessments. The type of assessment chosen by the team depends on the type of mission.

The first assessment option is a written test, which is preferable for short missions conducted in a classroom setting. This approach is not always ideal, because language barriers can inhibit clear test translation; additionally, some partner nation trainees are averse to formal testing. A second assessment option is a practical application, which is ideally suited for longer missions requiring extensive field skills and infantry tactics training. This assessment model should be designed similar to the combat endurance test at the Marine Corps Infantry Officers Course, with separate skills stations and rigorous physical fitness tests. The benefit of this approach is that it avoids the appearance of formal testing while providing greater flexibility for trainers to evaluate the performance of partner nation military personnel. The disadvantages of this approach are two fold: first, the practical application assessment introduces more subjectivity into the evaluation process; and second, it requires additional trainers and larger training facilities, both of which may not be readily available.

A third assessment option is the combined approach, which incorporates elements of a written test with a practical application. This approach is ideally suited for multifaceted security cooperation missions that require a combination of academic training and field skills. This third assessment option encourages trainers to generate both quantitative and qualitative mission data while catering to a wider variety of learning styles.

Conventional Training and Readiness Evaluation Process

The conventional approach to evaluating partner nation forces is centered on the Marine Corps Training and Readiness Standards and Performance Evaluation Checklists (PECLs). PECLs include conditions, standards, and event components, which are evaluated by trained instructors. During the author’s deployment, the most common PECL used was a standard infantry patrolling checklist that included 15 event components (figure 2). During the course of an **[FIGURE 2 OMITTED] [FIGURE 3 OMITTED]** evaluation, the trainer first marks “yes” or “no” next to the “observed” column on the checklist. As each event component is completed, the evaluator will determine if performance is “Sufficient” (S) or “Insufficient” (I). After determining the average score for each of the event components, the trainer assigns a grade of “untrained,” “partially trained,” or “trained.” Most Marines are familiar with this evaluation process and are accustomed to using PECLs as a baseline for monitoring improvement. The problem with implementing a conventional approach to evaluations is that it ignores the nuances of host nation training requirements. The conditions, standards, and event components of traditional PECLs should be adjusted to reflect the requests of the host nation.

A Hybrid T&R Evaluation Process

Figure 3 represents an example of a hybrid PECL, which replaces event components 4 and 13 and adds event component 16 (hybrid adjustments are highlighted gray). The hybrid PECL provides a standardized template that is adjusted to meet the demands of the partner force.

First Lieutenant Robert Curtis used the methodology during a deployment with SPMAGTF-CR-AF 18.1. As the logistics combat element TSC coordinator, he experienced firsthand the utility of employing hybrid PECLs. According to First Lieutenant Curtis, “Using regular T&R standards is difficult because the partner nations are not equipped or organized like the Marine Corps; therefore, our standards do not always apply to them. Using hybrid T&Rs allows the teams to produce more focused and relevant assessments for the partner nation.”14

Process for Generating Assessment Data

After completing the nine-step methodology, the security cooperation team will be able to produce valuable quantifiable data that will shape future engagements. To produce this data, team leaders will need to complete a simple formula (figure 4). First, the team leader will compile the results from the initial assessment and compute the average for each student who was evaluated on a written test, a practical application test, or a combined test. In the case of the assessment data provided in figure 4, the average score is 48 percent. The team leader will then compile the results of the final assessment—ensuring the same test is used for both the initial and final assessment—and compute the average of the scores using either a mean or median calculation model. In the hypothetical illustration below, the final assessment average is 87 percent. The team leader will then compare the initial assessment with the final assessment and derive the absolute value or range of improvement for the mission. In the example provided in figure 4, the total range of improvement equates to 39 percent.

The data presented in figure 4 is representative of one security cooperation **[FIGURE 4 OMITTED]** mission, so regional planners who are responsible for multiple missions should collate the assessment data in a bar chart or bar graph format to depict the range of improvement across all missions during a given period of time as seen in the data presented during the SPMAGTF-CR-AF 17.1 TSC missions (figure 5).

Arguments in Support of the Hybrid Training and Readiness Assessment Methodology

Perhaps the most compelling reason to enact the methodology is to promote fiscal accountability and responsibility within the Marine Corps and the DOD. Among the Services, the Marine Corps is known for its propensity to conserve scarce resources. In the early nineteenth century, Commandant Archibald Henderson popularized the long-held Marine Corps mantra of “fighting on the cheap.”15 Henderson successfully lobbied for Marine Corps involvement in the Seminole Wars (1817–18, 1835–42, 1855–58) and the Mexican War (1846–48) largely because he was able to convince the president that the Marine Corps could accomplish the mission with fewer resources than the Army.16 A similar mentality persists in the modern Marine Corps. During a deployment in 2017, Marines with SPMAGTF-CR-AF saved approximately $700,000 in a $3,000,000 operational budget by implementing the aforementioned assessment methodology. Other Marine Corps units that employed the methodology during SPMAGTF-CR-AF rotations also garnered considerable cost savings. The data produced during these deployments equipped senior leadership with **[FIGURE 5 OMITTED]** the information necessary to eliminate extraneous programs and increase overall efficiency. By broadly integrating the Hybrid T&R Assessment Methodology into all partner nation engagements, the Marine Corps will further establish its reputation as a force that is ruthlessly efficient and frugal.

In addition to promoting fiscal responsibility, the methodology will also enhance planning across the tactical, operational, and strategic levels of war. In a recent Rand Corporation study, researchers identified several challenges facing the DOD as it continues to implement the AM&E framework. One particularly daunting challenge mentioned in the report is the process of comparing tactical security cooperation activities with U.S. policy objectives and determining if the activities have fulfilled the objectives.17 The authors of the study suggest that “a standardized [assessment, monitoring, and evaluation] AM&E regimen applied across activities helps policymakers and implementers make more informed decisions that maximize immediate outcomes and help ensure programmatic sustainability and impact in the longer term.”18 The report also mentions that assessments can provide important insight for planners: “If fully implemented, partner country capability/interoperability assessments have the potential to provide useful information to security cooperation planners and programmers who lack domain expertise or Service perspectives on what is needed from partner militaries.”19 Military planners are often criticized for their failure to harmonize the strategic, operational, and tactical levels of war. The methodology makes progress in achieving a more integrated approach to TSC planning.

Counterarguments

Despite the many benefits of adopting the methodology, there are also some drawbacks. One potential problem with the methodology is that it can create a culture of chasing the data, where security cooperation teams and partner forces are motivated by test performance at the expense of genuine teaching and learning. Although this challenge is worth consideration, it is not enough to overcome the need for assessments. When properly trained, security cooperation instructors recognize that assessments are only one aspect of effective education. A healthy educational culture is established by team leadership, and trainers must be willing to adjust the format and frequency of the assessments to prevent unhealthy obsession about data. One method for reducing the focus on assessments during partner force engagements is to ensure that the assessment results are anonymous. Reflecting on his time as a security cooperation team leader in Gabon and Ghana in 2017, First Lieutenant Brendan Gallahue summarized his approach to testing: “At the end of the initial assessment, we debriefed the group on how they performed and explained the average score for the collective unit, without posting each individual’s scores.”20 Security cooperation teams can mitigate an unhealthy assessment culture by promoting groupwide improvement and retaining close control of assessment results.

Another counterargument is that the Marine Corps lacks the capacity to fully train security advisors on more complex hybrid T&R standards. Purveyors of this point of view claim that the predeployment workup cycle is already limited for the SPMAGTFs and Marine Expeditionary Units (MEUs), and therefore units will not have the bandwidth to conduct ancillary security cooperation training. While some hybrid standards may require additional training, most of the hybrid PECLs include material that is familiar to conventional Marine Corps units. If more complex hybrid standards cannot be taught organically by individuals from a deploying unit, the unit can request individual augments to fill low-density skill sets. During previous security cooperation engagements, Marine units have successfully requested support from 2d Reconnaissance Battalion and 2d Combat Engineer Battalion to provide specialized skills training.

First Lieutenant Gallahue confirmed the feasibility of training security cooperation advisors and noted that his team was able to seamlessly integrate the methodology into their training plan. After his mission, First Lieutenant Gallahue observed that “using the Hybrid T&R Assessment Methodology actually made the mission execution a lot simpler than we anticipated. My team successfully built a training program around an initial assessment, where we established a baseline and culminated with a final exercise to measure the progress of our partners and gauge the effectiveness of the training.”21 The methodology is likely to cause some friction initially, but it will ultimately simplify the efforts of security cooperation trainers.

Summary

Anecdotal, experiential, and empirical evidence all suggest that the Marine Corps and DOD support the need for a tactical-level assessment methodology. Despite repeated mandates from Congress to account for the billions of dollars’ worth of security cooperation expenditures, only marginal progress has been achieved. At this point, the return on investment for the security cooperation enterprise is unclear, at best. The Hybrid Training and Readiness Assessment Methodology is a tool that can radically shift the investment proposition of the enterprise from one marked by tepid returns to a position of maximum return. The methodology fills a critical role in connecting tactical, operational, and strategic planning while also promoting fiscal responsibility and accountability. Sherlock Holmes’ famous aphorism summarizes the problem and the potential solution for what ails security cooperation efforts: “It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.”22 Indeed, by leveraging facts and data, the security cooperation enterprise will transition from seeking alpha to at last achieving alpha.

#### Presume their solvency advocates are wrong absent AM&E – overwhelming empirical failure should make you extremely skeptical that implementation will meet expectations

Munson 13 Peter J. Munson, senior vice president for preventive services and global crisis management for a private sector corporation, retired U.S. Marine Corps officer, “The Limits of Security Cooperation,” War On The Rocks, 9-10-2013, <https://warontherocks.com/2013/09/the-limits-of-security-cooperation/> /GoGreen! \*added [warrantless]

As the Arab world continues to unravel, violence re-escalates in Iraq, and withdrawal from Afghanistan portends, this appears to be a good time to consider U.S. security cooperation (SC) policy. Security cooperation is a cornerstone of U.S. defense strategy, especially as the Department of Defense looks ahead at attenuated budgets and force structure. Planners imagine that security cooperation is a force multiplier; a way to do more with less. At face value, it extends U.S. influence and enables and influences partners to foster and improve security in their region, forestalling crisis, and replacing U.S. presence with like-minded regional guardians of the international status quo. While the idea makes much sense in the abstract, once it collides with the messy reality of military institutions and domestic politics in the world’s most troubled region, it becomes sometimes comically, sometimes disastrously, out of touch with reality.

Security cooperation is defined in the Security Assistance Management Manual as,

all activities undertaken by the Department of Defense (DoD) to encourage and enable international partners to work with the United States to achieve strategic objectives. It includes all DoD interactions with foreign defense and security establishments, including all DoD-administered Security Assistance (SA) programs, that build defense and security relationships; promote specific U.S. security interests, including all international armaments cooperation activities and SA activities; develop allied and friendly military capabilities for self-defense and multinational operations; and provide U.S. forces with peacetime and contingency access to host nations. It is DoD policy that SC is an important tool of national security and foreign policy and is an integral element of the DoD mission.

The problem with SC is that it is implemented as if all of the aforementioned positive results are a given in every situation. In reality, positive results are exceedingly rare with the most challenging and troubled partners—the very situations for which officials desperately hope SC to work miracles. While officialdom is unlikely to admit the bankruptcy of many-to-most SC efforts, the time is now to reconsider the blind [warrantless] faith in SC as the wave of the future.

There are two general rationales for conducting SC. On one hand, U.S. forces seek to increase the capabilities of foreign partners and their ability to interoperate with U.S. and coalition troops. On the other, SC is seen as a tool to gain and maintain access to key leaders and critical facilities in foreign nations, providing the toehold before the toehold needed to enable contingency response. This idea of gaining access through SC can also be expanded to gaining influence over foreign partners due to close and continuing SC relationships. Unfortunately, the reality generally falls far short of the ideal in both cases.

When it comes to capacity building, efforts are all too often wasted. In a limited number of cases—predominantly with more elite units trained by special operations forces and in a few partner countries serious about developing their military—capacity building works well. In the remainder of cases, capacity building efforts are an exercise in futility as evinced by the numerous cases in which decades of SC have yielded no perceptible change in the capabilities of partner militaries. Individual and unit skills remain abysmal and despite high-dollar purchases of prestige weaponry, these militaries are generally unable to conduct routine maintenance, logistical, and training functions despite SC campaigns designed to enable these critical supporting capabilities. As a result, warehouses become dusty trophy cases of expensive U.S. military equipment that is either unusable due to poor maintenance status, or ineffective due to the lack of trained operators and command and control capabilities.

#### Turns solvency – implementation will be ineffective or counterproductive

Pretelt 21 Maj. Carlos De Castro Pretelt, U.S. Army, Foreign Area Officer serving as the Operations Section Chief at the Office of Defense Coordination in Mexico City, MA International Policy and Practice, George Washington University, MA International Management, University of Phoenix, BS social psychology, Park University, “Taking a Bite out of the Elephant: How to Improve Security Cooperation,” Small Wars Journal, 7-17-2021, <https://smallwarsjournal.com/jrnl/art/taking-bite-out-elephant-how-improve-security-cooperation> /GoGreen!

Measuring the effectiveness of security cooperation has long been an elusive, pervasive and complicated ordeal. Due to congressional guidance, there is a building impetus to ameliorate the established approach and develop new ways to meet this challenge. To remain relevant, security cooperation practitioners must become creative, methodical, and rigorous in their assessments of past and future initiatives to unambiguously demonstrate the positive impact of their proposals. Customized training will go a long way towards addressing this, but there will also have to be organizational changes. Security cooperation is an important program that grants the DoD the opportunity to develop stronger bilateral ties with partner nations and strengthen alliances. Unfortunately, its effectiveness has greatly varied due to the frequent creation of poorly justified and/or planned initiatives that oftentimes have no discernable long-term effect, at best, and, at worst, create more security challenges for our partners.

#### Turns solvency – failure to assess makes implementation counterproductive

Tankel 15 Stephen Tankel, nonresident scholar at the Carnegie Endowment and assistant professor at the School of International Service at American University; and Dafna Rand, former deputy director of Studies and Leon E. Panetta fellow at the Center for a New American Security; “Security Assistance Isn’t the Quick Fix the US Thinks It Is,” Carnegie Endowment for International Peace, 8-6-2015, <https://carnegieendowment.org/2015/08/06/security-assistance-isn-t-quick-fix-us-thinks-it-is-pub-60977> /GoGreen!

Security assistance and cooperation has been a critical pillar of U.S. statecraft for decades. The post-9/11 interest in using assistance and cooperation to incentivize and enable local partners contributed to the creation of a slew of new authorities and programs. Yet, despite its strategic centrality and large price tag, our report argues that many security assistance and cooperation programs fail to achieve U.S. objectives because of strategic and structural deficiencies.

Strategically, U.S. policymakers are often not clear about the specific outcomes they intend to achieve with security assistance and cooperation. Even when objectives are clear, there may be too many of them for a single program, which results in conflicting objectives. This is especially troublesome when pressing, short-term objectives subvert long-term U.S. goals. Also, there is currently no system in place to adequately assess outcomes. This not only risks wasting taxpayers’ dollars. Failure to assess progress and adjust programs accordingly can actually reduce U.S. influence with recipient states, which may believe they can free-ride or begin to view assistance as an entitlement. The practice of using security assistance to build relationships sometimes contributes to this problem. So does the fact that policymakers too often look to security assistance as a quick fix or way to address demands to “do something.”

### AT: AM&E Fails

#### Even if not methodologically, it’s politically key to prevent Congressional defunding

Pretelt 21 Maj. Carlos De Castro Pretelt, U.S. Army, Foreign Area Officer serving as the Operations Section Chief at the Office of Defense Coordination in Mexico City, MA International Policy and Practice, George Washington University, MA International Management, University of Phoenix, BS social psychology, Park University, “Taking a Bite out of the Elephant: How to Improve Security Cooperation,” Small Wars Journal, 7-17-2021, <https://smallwarsjournal.com/jrnl/art/taking-bite-out-elephant-how-improve-security-cooperation> /GoGreen!

Measuring the effectiveness of security cooperation has long been an elusive, pervasive and complicated ordeal. Due to congressional guidance, there is a building impetus to ameliorate the established approach and develop new ways to meet this challenge. To remain relevant, security cooperation practitioners must become creative, methodical, and rigorous in their assessments of past and future initiatives to unambiguously demonstrate the positive impact of their proposals. Customized training will go a long way towards addressing this, but there will also have to be organizational changes. Security cooperation is an important program that grants the DoD the opportunity to develop stronger bilateral ties with partner nations and strengthen alliances. Unfortunately, its effectiveness has greatly varied due to the frequent creation of poorly justified and/or planned initiatives that oftentimes have no discernable long-term effect, at best, and, at worst, create more security challenges for our partners.

#### It’s powerfully effective

Marquis 16 Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; S. Rebecca Zimmerman, Policy Researcher at RAND; Merrie Archer, Senior Pol-Mil Policy & Plans Advisor, Bureau of Political Military Affairs, U.S. Department of State, MA International Affairs, Economic and Political Development, Columbia University; Jeremy Boback, assistant policy researcher at RAND; and David Stebbins, senior policy analyst at RAND; “Developing an Assessment, Monitoring, and Evaluation Framework for U.S. Department of Defense Security Cooperation,” RR1611, RAND Corporation, 2016, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1611/RAND_RR1611.pdf> /GoGreen!

AME focused on measuring and improving return on investment is a powerful tool for strategic decisionmaking, including resource allocation in support of current and future programs and activities. A standardized AME regimen applied across activities helps policymakers and implementers make more informed decisions that maximize immediate outcomes and help ensure programmatic sustainability and impact in the longer term.

Although the thrust of the AME effort is still being determined within the Office of the Secretary of Defense (OSD) and the Joint Staff, there are indications of the direction in which important elements of DoD would prefer to head. Interviews conducted by officials in OSD in 2015 with security cooperation stakeholders, decisionmakers, and practitioners throughout DoD and within relevant interagency circles8 on their priorities for AME revealed an overwhelming concern with informing better outcomes now and improving future policy and programs, closely followed by improving utilization of security cooperation as a tool and informing resource allocation decisions.

#### Empirics prove

McNerney 16 Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland, “Department of Defense and Security Cooperation: Improving Prioritization, Authorities, and Evaluations,” testimony before the Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, U.S. Senate, 3-9-2016, <https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT454/RAND_CT454.pdf> /GoGreen!

Evaluation is the ultimate goal of AM&E and requires that all other components work well. Providing a piece of equipment or training a military officer is not an end unto itself. Investments require following up to make sure that they yield the full potential benefits that were expected. Many organizations inside and outside the U.S. government have put a heavy emphasis on the ability to evaluate progress toward objectives. The Gates Foundation and World Bank have been trailblazers in this field. The Millennium Challenge Corporation, U.S. Agency for International Development, and State Department have all found at least some success in evaluations, even in areas that are not amenable to quantifiable metrics. Within DoD, the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict oversees a promising evaluation process for its Section 2282 Train and Equip program.

In the case of the Section 2282 program, DoD uses a small team of independent outside evaluators who have established reasonable, common standards of capability and performance for the types of missions supported by this authority. These standards are applicable to all partner nations that receive assistance. The team visits the recipient partner organizations about one year after training and equipment is provided, both to monitor use of the assistance and to evaluate the effects of that assistance. Results— the good, the bad, and the ugly—are consolidated into an annual report that highlights key points for the Secretary of Defense to transmit to Congress. The teams have been to 20 countries in the past four years and have documented their approach in a handbook to ensure consistency of application.

RAND is working with DoD to help it apply lessons from various organizations and create a framework that can be applied across the entire department to establish roles and responsibilities for managing AM&E more effectively. We hope this will support Congress’s requirement in Section 1202 of the 2016 National Defense Authorization Act for DoD to issue a strategic framework prioritizing security cooperation resources and activities.

#### They can’t pretend the details of SC don’t matter – they’re AFF! – we know it CAN work – the question is what will get resourced

Shah 18 Hijab Shah, research associate with the International Security Program at the Center for Strategic and International Studies (CSIS); and Melissa Dalton, senior fellow and deputy director of the CSIS International Security Program; “Security Cooperation as a National Defense Strategy Tool,” Commentary, 10-3-2018, <https://www.csis.org/analysis/security-cooperation-national-defense-strategy-tool> /GoGreen!

Security cooperation has long been a vital tool of U.S. foreign policy. The 2018 National Defense Strategy (NDS) elevates its importance. “Strengthening alliances and attracting new partners” is one of the three pillars delineated in the NDS as a major line of effort against strategic competitors such as Russia and China. As the United States evolves its global approach in the face of increasingly complex security challenges, the U.S. government may find that it is more reliant than ever on allies and partners in the pursuit of shared security goals in key conflict theatres and broader regions of interest. This will involve a spectrum of activities including institutional capacity building, training, exercises, education, and arms sales, to meet operational, transactional, and broader foreign policy objectives. Historically, this has been a source of strength for the United States, building a network of partners and allies to address common problems beyond which the United States may be able to accomplish alone. Security cooperation is thus a way to ensure U.S. superiority in this era of strategic competition. However, countervailing priorities in the current U.S. administration challenge this formulation. In addition, questions remain as to how the Department of Defense—and more broadly, the U.S. national security interagency—will organize for and resource the strategic application of security cooperation.

### AT: AM&E Fails – Chasing Data

#### Bad metrics are exactly what’s wrong with current practices – AM&E is the solution

Pretelt 21 Maj. Carlos De Castro Pretelt, U.S. Army, Foreign Area Officer serving as the Operations Section Chief at the Office of Defense Coordination in Mexico City, MA International Policy and Practice, George Washington University, MA International Management, University of Phoenix, BS social psychology, Park University, “Taking a Bite out of the Elephant: How to Improve Security Cooperation,” Small Wars Journal, 7-17-2021, <https://smallwarsjournal.com/jrnl/art/taking-bite-out-elephant-how-improve-security-cooperation> /GoGreen!

Elusive and Misunderstood

It is difficult to ascertain if a security cooperation initiative is effective or not.[iii] This could be in part because most of the indicators of success used by security cooperation stakeholders may not be focused on measures of effectiveness, but of performance, i.e., quantity of equipment delivered and number of units trained. As one begins to peel back the layers of an initiative, it becomes apparent that the necessary in-depth analysis which forecasts secondary and tertiary orders of effect may have been overlooked, along with critical, measurable metrics that explain how an initiative would specifically elicit a proposed reaction. The example utilized by Maj Croshier described the unanticipated difficulties of providing a C-208 fixed-wing reconnaissance aircraft and Command and Control (C2) equipment to Niger, Chad, and Cameroon. The focus of this initiative was placed mainly on the equipment, without fully accounting for the significant personnel, doctrinal, and maintenance challenges that would ensue.

It is also worth highlighting that these types of issues are not solely to the DoD. A few years back, the Department of State’s Bureau of Political-Military Affairs, Office of Security Assistance (PM/SA), created an Assessment, Monitoring, and Evaluation (AM&E) team to evaluate the efficacy of Foreign Military Sales (FMF) and International Military Education and Training (IMET). This year, the team released a study that found that initial reporting from the field demonstrated various issues with the way FMF is being implemented. In particular, a lack of understanding of the long-term maintenance requirements for military equipment grants.[iv] The report also mentioned that most of the current initiatives do not sufficiently take into account the economic viability of a partner nation. This often results in the partner nation feeling forced to keep the donated equipment operational, straining their maintenance budget and reducing their funding for other programs. This generates negative consequences for the bilateral relationship and potentially creates additional security challenges for the partner country.

The Million-Dollar Paperweight

Unfortunately, as mentioned above, it is difficult to ascertain if a security cooperation initiative has achieved its objective solely by measuring the delivery of equipment. This is due in part to the use of subjective measurements to evaluate them, such as narratives, and the still nascent and limited implementation of standardized AM&E efforts. However, based on the recurrence of this issue and the results from the Bureau of Political-Military Affairs, Office of Security Assistance (PM/SA) report, one could deduce that perhaps the root of the problem is an overreliance on military equipment grants by security cooperation practitioners. And, although it’s hard to pinpoint why exactly, there could be a very simple reason why stakeholders prefer this option. The most likely answer is because the system itself is built to reward those who demonstrate something measurable happened during their evaluation period.

Whereas developing a strategic bilateral document could substantially help mature a bilateral relationship, it could take years to accomplish and there is no guarantee it will come to fruition. Amongst security cooperation stakeholders, ordering equipment is a far less risky endeavor with a substantially higher chance of completion. The problem is that the equipment itself is seldom the answer to complex security challenges. For every piece of equipment, there must be a sizable support footprint that ensures its continued operation. Far too often, security cooperation practitioners become fixated on the metrics associated with the number of individuals trained or the costs of the equipment donated, not fully understanding if either the training or the equipment will demonstrably resolve the security challenge.

#### “Chasing data” problems are solved in implementation – our link outweighs

Van Eerden 20 Captain James R. R. Van Eerden, deputy director, chief operations officer, and Marine detachment officer-in-charge, National Security Agency, graduate of the Expeditionary Warfare School, Marine Corps University, “Seeking Alpha in the Security Cooperation Enterprise: A New Approach to Assessments and Evaluations,” Journal of Advanced Military Studies, 11(1), Spring 2020, DOI 10.21140/mcuj.2020110105, pp.113-126 /GoGreen!

Despite the many benefits of adopting the methodology, there are also some drawbacks. One potential problem with the methodology is that it can create a culture of chasing the data, where security cooperation teams and partner forces are motivated by test performance at the expense of genuine teaching and learning. Although this challenge is worth consideration, it is not enough to overcome the need for assessments. When properly trained, security cooperation instructors recognize that assessments are only one aspect of effective education. A healthy educational culture is established by team leadership, and trainers must be willing to adjust the format and frequency of the assessments to prevent unhealthy obsession about data. One method for reducing the focus on assessments during partner force engagements is to ensure that the assessment results are anonymous. Reflecting on his time as a security cooperation team leader in Gabon and Ghana in 2017, First Lieutenant Brendan Gallahue summarized his approach to testing: “At the end of the initial assessment, we debriefed the group on how they performed and explained the average score for the collective unit, without posting each individual’s scores.”20 Security cooperation teams can mitigate an unhealthy assessment culture by promoting groupwide improvement and retaining close control of assessment results.

#### Results will be communicated and change decision-making behaviors

Yayboke 19 Erol Yayboke, senior fellow with the International Security Program and director of the Project on Fragility and Mobility at the Center for Strategic and International Studies, teaches global fragility and resilience at the Maxwell School of Citizenship and Public Affairs at Syracuse University, MPA, BBA international business, University of Texas at Austin; MacKenzie Hammond, research associate at CSIS; Hijab Shah, research associate at CSIS; and Melissa Dalton, senior fellow and deputy director of the CSIS International Security Program; “Assessment, Monitoring, and Evaluation in Action for Security Sector Assistance,” Commentary, Center for Strategy and International Studies, 6-27-2019, <https://www.csis.org/analysis/assessment-monitoring-and-evaluation-action-security-sector-assistance> /GoGreen!

Communicating Results to Affect Change

With competing priorities diverting the attention of the U.S. leadership away from SSA, SSA implementers should communicate results effectively. Doing so can affect positive change in AM&E for SSA programming; it can also have implications for resourcing. Strategically, connecting SSA goals to broader U.S. policy objectives and framing success from that lens is one way to accomplish this. It requires not only reconciling potential mismatches in objectives between the programmatic and strategic level but also to establish a common and cohesive operating framework and vision between planners and implementors, bridging the gap internally before then communicating with U.S. government leadership. Incorporating these elements into AM&E for SSA will serve not only as a forcing function for the SSA bureaucracy to get its house in order but could also provide examples of progress and success that can be shared with policymakers to affect change. Better AM&E for SSA can help the community tell its story more effectively.

Facilitating dialogue and communication within the interagency will be just as important as doing so with Congress. The interagency AM&E community must also work on better utilizing its monitoring data to inform course corrections and, one step further, communicate the process and results effectively to the strategic level. This will help illustrate the connection between programs and foreign policy goals at the country and regional level for Washington-based policymakers. This should also include communicating behavioral changes and perception changes to understand locally legitimate authorities and how trust is shifting on-the-ground. Taking advantage of moments of political and policy transition is also critical and will require leadership and coordination between the higher echelons of the SSA interagency. AM&E can provide real time feedback to make this coordination easier and more efficient.

Finally, communicating SSA results using the return on investment paradigm may create a greater impact amongst policymakers. The U.S. SSA community should leverage AM&E in a way that communicates the rewards of SSA programming reaped by the United States. This method should include demonstrating U.S. dollars are being put to good use through measurable progress in areas such as increased capacity and capability within the recipient country, improved political will to correct certain behaviors, co-investing from within the recipient country or through outside allies and partners, and the overall quality of recipient engagement.

#### Trying is better – gut checks are worse

McNerney 16 Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland, “Department of Defense and Security Cooperation: Improving Prioritization, Authorities, and Evaluations,” testimony before the Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, U.S. Senate, 3-9-2016, <https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT454/RAND_CT454.pdf> /GoGreen!

Make no mistake: Working with foreign militaries is more art than science. But it certainly shouldn’t be abstract art. Security cooperation is most effective when it’s based on coordinated planning and informed by rigorous analysis. But ultimately, it must be tailored by the dedicated men and women serving overseas to meet the realities they face on the ground. Clear guidance and intensive training are crucial to ensure that they can overcome the many challenges that arise in this line of work.

#### Our ev also answers the complaint about diagrams

McNerney 16 Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland, “Department of Defense and Security Cooperation: Improving Prioritization, Authorities, and Evaluations,” testimony before the Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, U.S. Senate, 3-9-2016, <https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT454/RAND_CT454.pdf> /GoGreen!

Addressing the challenges of evaluation also requires breaking down the process of evaluation into its component parts, which we think of as “AM&E”: baseline assessments, monitoring of performance, and evaluations of effectiveness. But before looking at AM&E—and this relates to my earlier point about prioritization—senior leaders must decide what is worth measuring. In command headquarters in Afghanistan, Germany, Iraq, Honolulu, and Tampa, I have seen massive slide presentations and spreadsheets analyzing various security cooperation activities until it all becomes a blur, and I surrender to the operations researchers and engineers who have designed them. How much more difficult is this process for congressional overseers who review an even greater scope of national security issues? These slides and spreadsheets may well be important for the organizations in which they reside, but evaluations must translate into something that can highlight a few key areas of progress and problems.

## !—COMPETITION

### AT: !/D – No GPC

#### Critics are wrong – competition is fact, NOT strategy, there’s no winning, merely managing to survive

Shaw 21 Ryan Shaw, Senior Advisor and Professor of Practice in History and Strategy at Arizona State University, PhD, MA history, Yale University, BA American Government and Politics, US Military Academy at West Point, “In Defense of Competition,” Real Clear Defense, 11-11-2021, <https://www.realcleardefense.com/articles/2021/11/11/in_defense_of_competition_803143.html> /GoGreen!

As the Pentagon readies its new National Defense Strategy, the commentariat—unsurprisingly—has some thoughts. While the perspectives are, no doubt, as varied as the array of think tanks and universities from which they spring, there seems to be a significant piling on against both the “Great Power Competition” that animated Trump-era guidance and the (allegedly distinct) “Strategic Competition” terminology advanced by the Biden administration. But “competition” is a rare instance of bipartisan continuity because it speaks to real and important dynamics in the international system, and it has led to important new thinking in our approach to national security. We should not be so quick to discard it.

Rather than abandoning competition, it is time now to double down. The Pentagon strategy should embrace a robust concept of integrated deterrence, and the White House should lead with a National Security Strategy (NSS) rooted in a holistic approach to Competitive Statecraft.

The critics are right that Great Power Competition (“GPC”) has become a vacuous catch-all, a magic word, as CNAS’s Wasser and Pettyjohn tell it, that can justify “every force, capability, or resource request.” But that’s a perennial bureaucratic tendency; the same was true of CT and then COIN in the Bush and Obama years, and probably any number of terms du jour in prior eras. We should always work to minimize these abuses, but we won't eliminate them as long as we use words to describe our priorities. Other critiques are less valid and far less helpful.

The idea that an emphasis on competition precludes the possibility of cooperation is an unhelpful reductio ad absurdum. Pundits may not be able to sustain two competing ideas at once, but the international system always does, and the military clearly can: emerging U.S. doctrine envisions a competition continuum, in which “the joint force… campaigns through a mixture of cooperation, competition below armed conflict, and armed conflict calculated to achieve the desired strategic objectives.” As Daniel H. Nexon points out, “Even during the Cold War, the United States and the Soviet Union worked out a variety of formal and informal rules that helped them manage competition, limit nuclear proliferation, and otherwise structure international relations.” (It is unclear how Nexon intends this observation to support his argument against competition.)

Equally unhelpful is the common complaint that the phrase “‘strategic competition’ reflects uncertainty about what that competition is over and what it means to win.” Here again, while it might stymie the pundits, this intellectual hurdle seems not to have tripped up our military leaders—they have been consistent in identifying the stakes of this competition as the “rules-based international order that brought prosperity and relative peace for the last seven decades.”

And “what it means to win” is just the wrong question—that’s the whole point. Echoing George Kennan ("We have been handicapped … by a popular attachment to the concept of a basic difference between peace and war…"), the competition discussion is enabling the military to finally—against all odds—shed the idea of war as a finite game that starts with an opening salvo of munitions and ends with a ceasefire and a treaty. The fixation on “winning” breeds fatal short-termism—see the common refrain that we didn't fight a twenty-year war in Afghanistan, but rather twenty one-year wars.

What all these simplistic critiques miss is the simple old truth that the enemy gets a vote. Nexon wants us to consider competition as a means rather than an end. But it’s neither—it’s just a plain fact of our strategic environment, and the last round of guidance intended to highlight it as the most salient one for U.S. strategy. It may or may not have been true, but we operated for much of the last thirty years as though we did not have any real competitors, ideologically or materially. The “end of history” trope after the Cold War was premised on the absence of an ideological alternative to liberal democracy; and if 9-11 proved that wrong, the “asymmetric” modifier we appended to the “warfare” of the Global War on Terror reassured us that proponents of radical Islam lacked the resources to make their vision an existential threat.

But the long-term ascendency of liberal, democratic ideals and rules-based international order is neither inevitable nor irreversible. There are alternatives on offer, and they are actively being pursued by adversaries whose capabilities across many domains threaten to eclipse our own in the not-so-distant future. These are the facts, and they demand our attention. The last NSS and NDS were right to frame them that way.

We must prevent the loss of our competitive advantage and deterrent capacity in conventional and nuclear warfare—competition should not prevent that; properly conceived, competition demands it. (The Pentagon understands this, too.) But the most pernicious element of these arguments against competition is the insinuation—or the outright assertion—that we can or should focus on high-end capabilities to the exclusion of all else. This requires a willful disregard of everything we have learned about the gray zone/hybrid warfare/choose-your-appellation. After all, while our high-end advantage has eroded, it is not gone. We have so far deterred major conventional and nuclear war, but our adversaries—especially those near-peer “great powers”—have found countless ways to improve their strategic position and degrade ours without triggering a conventional military response. High-end deterrence is necessary, but it’s clearly not sufficient. The accumulation of minor setbacks can be existential, not just because of their obvious and immediate effects, but because they can degrade our long-term ability to generate and project conventional power.

For all its emphasis on GPC, the last NDS recognized the interrelated nature of threats at all points on the competition continuum. This was made especially clear in the Irregular Warfare Annex: “State adversaries and their proxies increasingly seek to prevail through their own use of irregular warfare, [suggesting] the need for a revised understanding of IW to account for its role as a component of great power competition.”

What we need is not a narrower concept of deterrence but a broader one that focuses not just on the future conflict we could lose but also on the ongoing competition we are currently losing. Perhaps this is where Secretary Austin’s nascent “integrated deterrence” idea is headed. He seems to want to integrate across domains and technologies and with allies, and who could argue? Well, lots of people, including Representative Mike Gallagher (R, WI), who has apparently been reading his Pettyjohn: “What we actually need to integrate is more conventional hard power—more ships, more long-range missiles and more long-range bombers in the Indo-Pacific.”

Gallagher here is giving voice to a perpetual false choice we frame between conventional and irregular capabilities. But as the IW Annex said, competing in the contested space “does not require significant new resources… it requires new ideas and new means of employing existing capabilities.” The limiting factor is not in our pocketbooks, it’s between our ears. Educating for IW may not lead to great photo-ops, but it could lead to better outcomes below the threshold of major war, which would be worth a great deal more. Unfortunately, after our inglorious exit from Afghanistan, it seems we are determined to repeat what the Annex called “the ‘boom and bust’ cycle that has left the United States underprepared for irregular warfare in both Great Power Competition and conflict.”

Some Congressional leaders are pushing back. Last year's NDAA included authorization to establish a DOD center for studying irregular warfare. This year's bill is still in draft, but both chambers have provisions demanding an implementation plan for the IW Annex, and the House bill would require a report on the establishment of the center. Educating for IW may not lead to great photo-ops, but it could lead to better outcomes below the threshold of major war, which would be worth a great deal more.

With all due respect to Secretary Austin, an integrated deterrence worth its name would be integrated both vertically and horizontally. Vertically, it would supplement our nuclear and conventional deterrence with unconventional deterrence to provide creative and seamless response options other than “do nothing” and “all-out war.” Horizontally, along with allies and partners, it would integrate military force with the other instruments of U.S. national power.

#### Fettweis is wrong – absence of competition and presence of effective US partnerships have greater explanatory power

Hoffman 15 Frank G. Hoffman, Senior Research Fellow at the Center for Strategic Research at National Defense University, former Senior Director, Naval Capabilities and Readiness, Department of the Navy, Lieutenant Colonel (ret.) US Marine Corps Reserve, PhD War Studies, King’s College, London, MA Security Studies, Naval War College, MEd George Mason University, “Just How Dangerous Is It Really?” War On The Rocks, 3-17-2015, <https://warontherocks.com/2015/03/just-how-dangerous-is-it-really/> /GoGreen!

In his recent Congressional testimony, the Director of the Defense Intelligence Agency, Marine Lt. Gen. Vince Stewart provided a worldwide threat assessment that noted “A confluence of global political, military, social, and technological developments, which, taken in aggregate, have created security challenges more diverse and complex than those we have experienced in our lifetimes.”

This judgment runs directly counter to the arguments in a new book with a question as its title: A Dangerous World? The central theme of this anthology is that perceptions of the threats the United States faces are unrealistic or manifestly exaggerated. The contributors to this anthology are commendably consistent on these points, to a fault. They want the country and the Pentagon to confront real threats rather than preferred demons and warn the reader to be leery about accepting the “revealed wisdom” about the dangers the people of the United States face. In that regard, this book is a healthy (but not entirely convincing) exercise in challenging longstanding threat perceptions.

The 16 chapters of this tightly edited volume are penned by an impressive array of American academics. One of the early chapters comes from the co-editor, Professor John Mueller, a member of the Hall of Fame of Congenital Contrarians. He has thrown a lot of cold water in his career on hyperbolic threat prognosticators. His essay on proliferation and terrorism is soundly presented but is limited to nuclear threats. Professor Mueller’s perspective on the implications of proliferation comes off as too narrow and far too optimistic. He is correct that the pace of nuclear proliferation has been slower than feared, but of course, this decrease did not happen organically. Rather it was the product of active policy measures to increase pressure on states. Mueller fails to give credit to the establishment of these norms or the explicit pressures placed on proliferating states. He is probably right that “the consequences of proliferation that has taken place have been substantially benign.” But I disagree that proliferation by North Korea or Iran is quite as benign as say India and Israel. Many analysts believe that strategic stability in the Second Nuclear Age is weakening, generating more rather than less danger.

As the current cover story in the Economist notes:

The new nuclear age is built on shakier foundations. Although there are fewer nuclear weapons than at the height of the cold war, the possibility of some of them being used is higher and growing. That increasing possibility feeds the likelihood of more countries choosing the nuclear option, which in turn increases the sense of instability.

Former American intelligence analyst Paul Pillar assesses the dangers of terrorism in his chapter. He observes, “The idea that substate disorder overseas threatens U.S. interest is rooted in the tendency of Americans to go abroad in search of monsters to destroy.” Pillar challenges the idea that every failed state is a “safe haven” for Al Qaeda to plot another 9/11. The notions of safe havens are far less significant, he notes “in an era of globalization and globe-spanning information technology in which planning, recruitment, and the direction of operations take place at least as much in virtual space as they do in physical space.” What Pillar does not address is groups like the Islamic State in Iraq and the Levant (ISIL) and Boko Haram who are now seizing and holding not just safe havens but large swathes of real estate. It’s not clear that the United States can defang ISIL since it is evident U.S. leaders do not understand it. But overall, until such groups challenge our core interests, Pillar rightfully argues the United States should not make matters worse.

Martin Libicki from RAND focused on cybersecurity, particularly our homeland security. Libicki notes that much of what concerns our society about cybersecurity is actually criminal behavior, not a true national security challenge. Even in his most speculative scenario of an attack on critical infrastructure, he does not estimate damages of $1 billion, which “is unlikely to be catastrophic – though the damage could be magnified considerably by hasty and ill-considered overreaction.” His views are consistent with other scholars including Kings College London lecturer Thomas Rid. While cybersecurity at home is overdone, Americans should be more pessimistic when it comes to military capabilities given the U.S. military’s huge reliance upon cyber connectivity and networked computer systems. U.S. forces are highly dependent on the secure use of IT-based systems for the conduct of operations, and remain vulnerable.

Joshua Shrifrinson and Sameer Lalwani offer a number of critical observations on maritime security. They note the United States has a sizable lead in maritime power over potential competitors and there are very few threats to freedom of the seas or direct threats to our ability to access the oceans. Shrifrinson and Lalwani attack the notion that the United States has an obligation to preserve freedom of access to the global commons for everyone else’s benefit. They effectively undercut the U.S. Navy’s stress on controlling the Global Commons, but their argument falls apart when then assert that competitors have little interest to contest U.S. command at sea or to seriously impact sea lanes of communication. The authors insist that no one will come close to U.S. capabilities for 20 years, and that China “lacks the ability, opportunity, or motivation to seriously challenge American command.” Instead of engagement and forward presence, their stated preference is for a more “hands off” approach that relies perilously upon regional actors. This is simply a form of off-shore balancing – what they define as “security of the commons.” The implication of this approach is that the United States could put a premium into convoy security, anti-submarine warfare, and missile defenses, while reducing forward presence onshore and our power projection forces. This approach, they contend, would “limit the spirals of insecurity that might cause challenges to American command to emerge, while pocketing the fiscal and political savings of a smaller footprint abroad.”

This argument fails to consider China’s own advances and its ongoing provocations in the Pacific, nor does it represent an understanding about how U.S. maritime dominance relates to our geopolitical interests or the reassurance of U.S. allies in the Pacific. Further, the authors do not satisfyingly explore the emerging combination of shore and sea-based cruise missiles in both the Pacific and the Persian Gulf. Several intelligence sources note Iran’s acquisition of more advanced capabilities including anti-ship cruise missiles and Chinese influence mines that will further complicate efforts to protect commerce in the Gulf. Rather than gut U.S. power projection and forward presence, the American people should realize that its Navy is dangerously smaller than it should be.

Christopher Fettweis of Tulane University wraps up the major contributors with a sweeping essay. To Fettweis, the world we live in today “is by all reasonable historical standards, a golden age of peace and security.” He continues, “The great powers seem to have given up fighting one another, and the lesser powers rarely go to war either, and levels of internal conflict are at all-time lows.” From his perspective there is an incontrovertible “growing mountain of evidence” that we live in an age where risks to our security are far lower than they are commonly thought. Habits of mind, hangovers from 9/11, and institutional constituencies are accorded as responsible for our “delusions of danger.”

Fettweis is perplexed by the prevalence of higher threat and risk perceptions held by many Americans, especially those in the national security establishment. Perhaps it is because “risk” is more than looking at the number of ongoing wars, where our policy has failed, or where interests are not engaged. Maybe it is related to perceptions of threats by policymakers from China, Russia, North Korea, and Iran that do not yet cross the threshold of war. Perhaps it is related to a deep understanding of human history and nature, rather than a truncated picture of the last generation where geopolitical pressures were at an all-time but transitory low. Perhaps it is because most of these countries have sharply expanded their military capacities and spending levels and expressed their intent to use their military forces rather than let them lie fallow. I’ve written in War on the Rocks before about the dangers of “culpable complacency.”

These shortcomings aside, readers will be impressed with the effort in A Dangerous World? and appreciate its contribution to a rigorous understanding of various threats. Several contributors score points in debunking myths. But the book did not alter my own assessment of the future for two reasons. First, too many of the authors tended to look backwards or focused in the present tense, and failed to extend threats into the future in a serious way. Potential challenges in the cyber and biotech domain come to mind, for example. When it comes to imagining our defense needs, we should look at trends with clear eyes and some imagination. One must examine trends and continuities, as well as projected discontinuities. Most of the authors in this volume were not so inclined. The combination of China’s assertiveness, Putin’s megalomania, the dawning of revolutions in cognitive, bioscience, and nanotechnology, and the socio-political eruptions of the Arab world, make a prudent strategist question assumptions about a constant glide slope to a peaceful and just world.

Second, I am inclined to see the progress of the last quarter-century as a deliberate byproduct of America’s ability to create and enforce a rules-based system with its allies, not as evidence of a global community that is inexorably marching along a linear and preordained path toward perpetual peace and shared prosperity. I do not discount progress but nor do I believe that it is self-generating, and am very skeptical it can be sustained in the absence of strong U.S. leadership. That linear pattern of reduced conflict totals, evident a few years ago, has flattened out and could worsen if we do not work to preserve our nation’s core security interests.

The conditions that generated those previously positive trends – lack of great power competition, reduced resource pressure, broad economic development, and generous support for conflict resolution are dissolving. In short, geopolitics, uneven economic development, human misery, and miscalculating leaders could ensure the return of history. Complacency and retrenchment on our part will only hasten it.

For a more future-oriented book, the National Intelligence Council’s Global Trends 2030 is a useful antidote to presentism. Matt Burrow’s new book The Future Declassified also looks at the future with balance, humility, and fidelity. Readers are encouraged to take a look at Chris Coker’s new book, The Improbable War, which warns about the dangerous pattern of thinking that a war with China is unlikely. On the Middle East, readers would do well to read any of the penetrating articles by Washington Post foreign affairs columnist David Ignatius.

While this book points out the dangers of careless Cassandras, we should not wear rose colored glasses as we peer into the future. It is not “pathologically parochial” to side, as I do, with General Dempsey’s latest statement to Congress and with retired Marine General James Mattis. The latter recently testified and emphasized that our position in the world is not self-sustaining. As former NSC and State Department official Nicholas Rostow has noted “Fundamental principles of world public order are at risk or directly challenged in Afghanistan, Ukraine, and the western Pacific,” and dire consequences for ignoring them.

The general theme of A Dangerous World? is that risks to our well-being and security are overstated, and security investments significantly reduced. That would be a huge error in my mind. Making that error would do more to completely undo what progress has been made and long peace we have enjoyed. I just see little justification as an historian for history to be cast as linear or evolutionary progress that moves inexorably only in one direction. We live in a better world right now, one which America’s influence and arms have helped shape. If we want to see positive trends continue it will not be achieved merely by retrenching our defense spending or retreating from the world stage. Stephen Pinker’s arguments notwithstanding, a true appreciation of history serves as a reminder of the folly of utopian thinking.

Overall, A Dangerous World? explored current threats and poked some holes at overhyped threats. It is strongly encouraged for classroom use in Security Studies programs since it promotes critical thinking. In the dangerous world we live in now and for the near future, we must see the world clearly. We need to separate true threats from routine problems, and differentiate between the unacceptable and the manageable. A Dangerous World? will help isolate the hype from the dangers we must fully confront.

## !—ALLIANCES

### AT: !/D – No Cred Theory

#### Perceptions of reliability matter – risks from BOTH abandonment and entanglement are real

Henry 20 Iain D. Henry, Lecturer at the Strategic and Defence Studies Centre, Australian National University, “What Allies Want: Reconsidering Loyalty, Reliability, and Alliance Interdependence,” International Security, 44(4), Spring 2020, pp.45-83, DOI 0.1162/isec\_a\_00375 /GoGreen!

This interdependence debate has usually focused on adversarial interactions and reputations for resolve, defined as “the extent to which a state will risk war to keep its promises and uphold its threats.” Loyalty is usually assumed to be the obvious “flip side” of resolve, and is not often studied in its own right.8 Some studies of reputation and alliances exist, but are predominantly focused on alliance formation rather than management.9 Because loyalty has not received the significant scholarly attention centered on resolve, alliance interdependence is undertheorized.10 But as the contemporary debate about Taiwan highlights, beliefs about loyalty and alliance interdependence could be a decisive influence on policy today. If alliance interdependence exists, scholars and policymakers urgently need to know how it works.

I argue that both the deterrence theorists and the reputation skeptics are wrong. Alliance interdependence exists—what happens in one alliance can affect others—but this is not determined by a national moral character of innate loyalty. When a state observes its ally's behavior in another alliance, it does not hope to see loyalty per se. Instead, it hopes to see proof that the ally's interests align with its own. In some cases, it will be in the observer state's interest for its ally to fulfill a separate alliance commitment—that is, the state will want its ally to be loyal to the other ally. But in other cases, where loyalty would not be in the observer state's interest, it will want its ally to be disloyal to the other ally. This reasoning contrasts starkly with other theories, which expect that a state will always want its ally to demonstrate inherent, pure loyalty. I argue that the state is unconcerned about whether its ally's behavior is loyal or disloyal in any objective or moral sense. Rather, when the state is confident that its ally's interests align with its own, and therefore the alliance poses no risk of either abandonment or entrapment, then the ally is reliable.11 Observed reliability—not innate loyalty—is what states want from allies. If an ally poses risks of entrapment, abandonment, or both, then it is unreliable, and the state will act to mitigate these risks. Responses could include hedging, diplomatic restraint initiatives, intra-alliance bargaining, threats of defection, attempts to entrap the ally, or, in extremis, alliance abrogation, bandwagoning, or nuclear proliferation.12

Deterrence theory recommends that states fight for reputation, and skeptics urge policymakers not to worry about reputation costs. I argue that adroit alliance management requires understanding how developments in one alliance can affect the reliability perceptions and behavior of other allies. The United States may need to fight—or not fight—to ensure that allies still perceive it as reliable. If the true nature of interdependence is recognized, the United States can manage alliance interdependence without being captive to a “cult of reputation.”13

In the first section of this article, I examine existing theories of reputation, loyalty, and alliance interdependence, and critique the belief that states want their allies to be indiscriminately loyal. In the second section, I explain why the concept of alliance reliability has greater explanatory power than the idea of loyalty. I propose hypotheses on reliability and alliance interdependence and contrast these with deterrence theory and Mercer's reputation-skeptic argument. In the third section, I use process tracing and archival research of the First Taiwan Strait Crisis (1954–55) to test my theory of alliance reliability. I show that although U.S. decisionmakers fretted about being perceived as disloyal to the Republic of China (ROC, or Nationalist China), most allies actively encouraged the United States to compel an ROC withdrawal from disputed territories and thus reduce the risk of conflict. In the final section, I summarize my findings and explain their implications for theory and policy.

## !—DEMOCRACY

### A/O – Demo !

#### AM&E’s key to global democracy – and reverse causal

Cole 21 Emily Cole, program officer for governance, justice and security in the Applied Conflict Transformation Center at the U.S. Institute of Peace, MALD Fletcher School at Tufts University, BA Amherst College; and Calin Trenkov-Wermuth, security governance advisor at USIP, formerly worked at the U.N. Office of Counter-Terrorism, served in the NATO Parliamentary Assembly, PhD, MA international relations, University of Cambridge, BA world politics Hamilton College; “To Consolidate Democracy, Change U.S. Security Assistance,” U.S. Institute of Peace, 12-16-2021, <https://www.usip.org/publications/2021/12/consolidate-democracy-change-us-security-assistance> /GoGreen!

Ample evidence—including the global surge in coups d’états and crises of police violence from Brazil and Nigeria to the Philippines—shows that dozens of countries must improve not only the “kinetic” capacities, but also their governance, of police, military and other security institutions. Yet a first outline last week of the new U.S. “initiative for democratic renewal” omits any mention of this vital task. The United States and its allies must re-shape their assistance to support democracy and human rights. In some countries—for example Egypt and Uganda—U.S. security sector assistance has helped to consolidate authoritarianism. Current trends risk exacerbating the problem in a “race to the bottom” among the United States, Russia and China.

U.S. policies too often set aside the nation’s commitment to democratic values on a flawed assumption that this is necessary to advance U.S. interests amid great-power competition. Yet democratic backsliding and authoritarianism create long-term risks of violence, instability and extremism. Even measured by the narrower metric of strategic military alliances, these risks weaken U.S. security interests. Serious democratic backsliding preceded Turkey’s decision to purchase one or more Russian S-400 missile defense systems. Democratic backsliding in the Philippines weakened the U.S.-Philippine security relationship to the point of endangering the agreement that has enabled a U.S. troop presence in the Philippines. Worldwide, democratic deficiencies help push countries into the arms of China or Russia.

How Security Assistance Can Hurt Democracies

The United States and others have historically ignored the significance of effective security sector governance for consolidating democracy. Donor countries have treated security sector reform as a technical problem, rather than a political endeavor that can change power dynamics and the political trajectory in a country. The recent coups in Sudan, Mali, Guinea, Myanmar and Chad show how an emboldened military and weak or absent civilian control over security forces may not simply weaken democracy, but end it.

To promote peace, stability, democracy and U.S. strategic objectives, the United States helps violence-afflicted nations with assistance to strengthen civil society, political parties, and legislative oversight. Yet the people overthrowing civilian, elected rule in Chad, Guinea and Mali this year were military officers who had been direct beneficiaries of U.S. training. This agonizing irony underscores that we can no longer neglect the central importance for democracy of helping nations improve security sector governance.

In these latest coups and in other examples, we see how security assistance itself can undermine democracy when it effectively “super-sizes” a vulnerable nation’s security services relative to weaker democratic, civilian institutions that are meant to control them. Where governments lack funding and capacities to meet populations’ basic needs, this danger skyrockets. Yet in too many cases—Egypt, Mali, Niger, the Philippines and others—U.S. and other security assistance has led to significant increases in military and security budgets at the expense of strengthening other critical services. Ill-balanced security assistance especially risks weakening democratic governance where it has backed major counterterrorism operations.

Egypt is a prime example. In the past four years, U.S. bilateral assistance to Egypt has been $1.4 billion per year, most of that to pay for Egypt to buy U.S.-made weapons. While this assistance has not enabled Egypt to end the threats from its terrorist groups in Sinai, it has buttressed the military regime, which now controls much of the country’s economy. Under current law and policy, only $300 million of the United States’ bilateral aid in FY 2021 was subject to being withheld by the State Department if Egypt failed to meet certain human rights and rule-of-law standards. The threat to withhold 23 percent of its assistance is far too little to show a powerful U.S. commitment to democracy, rights and governance. It reflects the relatively small amount that the United States has invested in promoting good governance.

President Biden often has said, “Don't tell me what you value. Show me your budget, and I'll tell you what you value.” This month, the Biden administration proposed spending up to $424.4 million next year on programs to strengthen democracy—an initiative that hardly compares to U.S. spending of roughly $18-20 billion each recent year on security assistance.

A Race to the Bottom

The United States’ current approach risks becoming a race to the bottom with China and Russia. In recent years, countries receiving security assistance have encouraged bidding wars among Russia, China, and the United States to seek the most attractive possible aid packages, including weapons. In fear of losing leverage over partners such as Philippines or Nigeria , the United States has participated. This allows authoritarian or authoritarian-leaning governments to procure weapons and other equipment and training for their militaries or police with little or no requirement for human rights or security governance improvements. In some cases, the fear of losing leverage may be unwarranted: After his initial flirtation with a closer relationship with China, Philippine President Rodrigo Duterte understood that China’s threat to his interests is very real and shifted back to the U.S. camp.

This means the United States has compromised on democracy and human rights for, at best, short-term gains in relations with a given country. In the long term, however, this approach undermines stability and democracy. During the Cold War, the U.S.’s primary goal of maintaining partnerships with governments in Africa to prevent them from absorbing Soviet influences yielded a similar approach. A RAND study concluded that “U.S. assistance appears likely to have increased the incidence of civil wars in this period, likely by either exacerbating domestic instabilities or provoking proxy conflicts.” There is no reason to believe that a 21st-century race to the bottom with Russia and China, in the interest of maintaining partnerships, will not have the same results.

We Can Do Better

The current U.S. approach to security sector assistance not only detracts from President Biden’s expressed goals of consolidating democracy and countering authoritarianism, it damages U.S. strategic interests in making it easier for China and Russia to engage with authoritarian regimes. As the United States builds from last week’s Summit for Democracy, it needs to fully apply, and in some cases expand, existing policies supporting democratic governance of the security sector. Key steps will include these:

1. Keep promises to withhold security assistance from human rights violators. Following through on existing legislation and keeping promises to withhold aid to bad actors is critical for the United States’ ability to support democracy abroad and for its credibility on the international stage. U.S. policy statements describe conditionality for aid—democratic governance and adherence to human rights norms—that often is ignored. As in Egypt, the United States often sustains security assistance to security partners even when countries fall far short of critical governance and human rights benchmarks. Frequently, senior U.S. officials may threaten to withhold aid, but without follow-through. This needs to change if democracy consolidation efforts are to have teeth.

2. Enforce assessment, monitoring and evaluation requirements. The 2017 National Defense Authorization Act required better assessment, monitoring and evaluation of security sector assistance. U.S. government officials admit that this is not happening yet, and big strides need to be taken to implement and learn from security assistance monitoring and evaluation. This is one way to ensure programming is effective and that it helps broader strategic objectives, including the consolidation of democracy.

#### Extinction

Haque 22 Umair Haque, economist, former director of the Havas Media Lab, degrees from London Business School and McGill University, “We’re Becoming a Far-Right Planet,” Eudaimonia and Co, 4-15-2022, <https://eand.co/were-becoming-a-far-right-planet-dc0487fa3b45> /GoGreen!

If It Feels Like the 1930’s Are Repeating Themselves — Only With Nukes — That’s Because They Are

There are two ways to think about the Russia’s bloody and brutal and criminal war in Ukraine. One is that Putin is a madman — with nukes. The second is even more chilling. It’s that Putin himself is a mere symptom, of deeper forces. These forces are vast and impersonal — just forces of history, like great currents beneath the waves of oceans. What do I mean? This second way to think — and the more that I reflect on it, the more accurate way, perhaps — goes like this.

We have many, many Big Existential Threats as a world. Climate change, mass extinction, ecological collapse, then pandemics, now nuclear war. But underlying all of these — and unifying them — is a deeply disturbing political reality. Over the last decade or two, the planet has swung so far right that it might as well have tilted on its axis. We are beginning to live on a far right planet.

And what kind of life, civilization, future is really possible on a far right planet? Not a democratic one. Not a peaceful one. It looks a lot like….this one. War, chaos, hate, rage.

This is a sea change. We haven’t lived on a far right planet for a long time. The last time we had hints of such a thing was in the 1930s. What’s happening today may be even more troubling, though, because it’s more widespread. I don’t think modern history — or even semi-modern history — has seen the entire planet swing far right so fast and hard that the globe is juddering in fear and agony.

Let me give you several examples of what I mean — and then I want to discuss why this is happening. We’ll start with rich countries — who are the obvious ones.

In America, it’s true, that Joe Biden’s President — but it’s truer that half the country or more is in open revolt against not just him, but the idea of liberal democracy. To teach kids that gay people exist is now a crime. Women’s rights are being taken away. Minorities are openly scapegoated. Yet another Black man was just shot in the head by a police officer…for nothing…on video. And shortly, every indication is that America’s conservatives are going to sweep into power, and reduce democracy to a shell, having laid the groundwork to snatch the election by whatever means necessary, from perverting electoral mechanisms, to another coup.

America’s new wave of laws attacking women and minorities and even teachers — tip lines, informants, secret polices — have roots in the Fugitive Slave Act, which deputised anyone to be a vigilante, and inspired the Nazis. That is how regressive its right wing revolt really is. America is therefore already ranked as a flawed democracy.

Take another set of rich Western countries, though. Britain’s head of state is literally now found to have broken the law. He didn’t resign. Instead, he came up with a plan to ship…refugees…to Rwanda…which is an authoritarian, totalitarian state whose record on human rights abuses is abysmal…and all that’s flagrantly against the law…again. None of this is remotely compatible with liberal democracy — from the rule of law to equality to justice to truth.

Then there’s Australia. Australians, deeply nationalistic people, think proudly of themselves as a liberal democracy, and fly into a rage when you criticise their nation. Yet the truth is their PM is a climate change denier, they pioneered the idea of human trafficking refugees to other countries — breaking international law — they have the highest per capita carbon emissions on the planet, and none of this seems to matter at all to them very much. Like Britain, for all intents and purposes, Australia is heading towards the far right. How else would you describe one whose PM denies climate change, while its ravaged by megafloods and storms and fires — and people just shrug?

In France, of course, Marine Le Pen is within striking distance of the Presidency. She comes from a family of proto-Nazi sympathizers, and openly backs Putin. Elected, she’d shred the West. She’s already called for NATO to effectively be broken up, and Frexit to happen. The EU would no longer exist as we know it. France is right on the brink of joining America, Australia, and Britain in hurtling towards far right politics.

Now, the rejoinder to all this will be: “At least we’re not Rwanda!!” But that isn’t the test of a liberal democracy. It’s whether, obviously, a nation is living up to the ideals of a democracy. Whether it values freedom, equality, truth, justice, decency, the rule of law, and so forth. It’s all too easy to see that in the cases I’ve presented to you, these things now have little value. When your head of state denies climate change — truth? LOL. When he breaks the law and covers it up by breaking the law — justice? LOL. When a society has tip lines to inform on neighbours for the crime of reading banned books — equality? Freedom? LOL.

This phenomenon stretches right around the world. It’s not just the rich world, the West, turning so far right that Adolf Hitler’s grinning approvingly, it’s also, obviously, the rest of it. Just two short decades ago, there were high hopes that Russia would evolve into a mature, stable, healthy democracy. Instead, it imploded into Putinism — and war. The same, more or less, is true in China and India. Across Asia and Africa and Europe, too. The planet is turning far right.

This is a scary thing. It has never really happened before. Yes, really, never.

Political scientists, scratching their heads, began to call this phenomenon “democratic backsliding.” But that turn of phrase is inaccurate. It implies that democracy is failing from both sides, left and right. We don’t live in an age, though, where the far left is overthrowing legitimately elected democracies. We live in one where the far right is. “Democratic backsliding” is therefore another way, really, to say — not say, in fact — “we are beginning to live on a far right planet.”

### AT: !/D – No DPT

#### Best studies disprove the confounding variables their ev cites and empirically confirm our impacts

Imai 20 Kosuke Imai, Professor of Government and of Statistics at Harvard University; and James Lo, Assistant Professor of Political Science at the University of Southern California; “Robustness of Empirical Evidence for the Democratic Peace: A Nonparametric Sensitivity Analysis,” International Organization, 75, Summer 2021, DOI 10.1017/S0020818321000126, pp.901-919 /GoGreen!

The democratic peace—the idea that democracies rarely fight one another— has been called “the closest thing we have to an empirical law in the study of international relations.” Yet, some contend that this relationship is spurious and suggest alternative explanations. Unfortunately, in the absence of randomized experiments, we can never rule out the possible existence of such confounding biases. Rather than commonly used regression-based approaches, we apply a nonparametric sensitivity analysis. We show that overturning the negative association between democracy and conflict would require a confounder that is forty-seven times more prevalent in democratic dyads than in other dyads. To put this number in context, the relationship between democracy and peace is at least five times as robust as that between smoking and lung cancer. To explain away the democratic peace, therefore, scholars would have to find far more powerful confounders than those already identified in the literature.

The proposition that democratic states do not fight interstate wars against each other is one of the most enduring and influential ideas in international relations. The idea is theoretically rooted in the work of Immanuel Kant, who argued that interactions between states with a republican form of government give “a favorable prospect for the desired consequence, i.e., perpetual peace.”1 This has led to a large literature empirically documenting a negative association between democracy and conflict,2 leading one scholar to comment that the democratic peace is “the closest thing we have to an empirical law in the study of international relations.”3

Despite the law-like nature of this association, no scholarly consensus has emerged on whether the observed association reflects a causal relationship or a spurious correlation. According to a recent survey, more than 30 percent of international relations scholars disagree with the democratic peace theory.4 In particular, skeptics have challenged the democratic peace by arguing that alliance structures from the Cold War,5 capitalism,6 and contract-intensive economies7 confound the observed association. These authors find that adding certain confounding variables to regression models eliminates the statistical significance of the estimated coefficient for the joint democracy variable.8

How should we resolve this empirical debate regarding the democratic peace?9 Unfortunately, in the absence of randomized experiments, we can never completely rule out the possible existence of confounding biases that arise from omitted variables. While scholars in this literature have exclusively relied on parametric regression models, this approach requires strong assumptions, namely that the model accurately characterizes the true data-generating process (correct set of variables, right functional form, valid distributional assumption, etc.). Given that these assumptions may not be verifiable from observed data, it is no surprise that various scholars advocate different regression models with diverging sets of variables, resulting in contradictory findings. The difficulty of adjudicating between these alternative modeling approaches has led to the ongoing controversy in the empirical democratic peace literature.

We propose an alternative approach based on nonparametric sensitivity analysis to formally assess the robustness of the empirical evidence.10 Specifically, we quantify the strength of confounding relationships that could explain away the observed association between democracy and peace. That is, we compute the precise level of unobserved confounding needed to render the observed association between democracy and conflict spurious. The idea is that although not all correlations imply causation, a very strong correlation suggests it. Unlike the parametric regression modeling approach prevalent in the literature, the proposed nonparametric sensitivity approach directly addresses the existence of unobserved confounders without assuming a particular regression model.11 Although one can never know with certainty from observational data whether democracy causes peace, this nonparametric sensitivity analysis can formally assess the robustness of empirical evidence for the democratic peace.

Our analysis applies the nonparametric sensitivity analysis method originally developed by Cornfield and colleagues, who were concerned with the robustness of the positive association between cigarette smoking and lung cancer in the potential presence of unobserved confounders.12 The study of the causal relationship between smoking and lung cancer closely parallels the dispute on the democratic peace. In both cases, randomized experiments cannot be conducted for ethical and logistical reasons, and critics contend that the observed association suffers from confounding biases. While no definitive conclusion can be drawn from observational data, Cornfield and colleagues argue that no existing confounder can explain the strong association between smoking and cancer and therefore this relationship is likely to be causal. Their conclusion is worth quoting here:

Cigarette smokers have a ninefold greater risk of developing lung cancer than nonsmokers, while over-two-pack-a-day smokers have at least a 60-fold greater risk. Any characteristic proposed as a measure of the postulated cause common to both smoking status and lung-cancer risk must therefore be at least nine-fold more prevalent among cigarette smokers than among nonsmokers and at least 60-fold more prevalent among two-pack-a-day smokers. No such characteristic has yet been produced despite diligent search.13

Our application of nonparametric sensitivity analysis to the democratic peace yields striking results. Depending on the definition of democracy, we find that a confounder must be at least forty-seven times more prevalent in democratic dyads than in other types of dyads. Thus, any potential confounder that could explain the democratic peace would have to be at least five times as prevalent as a similar confounder for smoking and lung cancer. In other words, according to our analysis, the positive association between democracy and peace is much more robust than that between smoking and lung cancer.

While no such confounder has yet been found for the relationship between smoking and lung cancer, we examine whether the confounders identified in the democratic peace literature meet the conditions of nonparametric sensitivity analysis. For example, we consider a set of economic confounders proposed by Gartzke who argues that the democratic peace can be explained by capitalism.14 We also consider other confounders, such as military alliances.15 Overall, our findings imply that for a potential confounder to explain away the democratic peace, it must be much more strongly associated with regime types and conflicts than the confounders that have been proposed to date. This finding again demonstrates the robustness of empirical evidence for the democratic peace.

Finally, we believe that a nonparametric sensitivity analysis, such as the one we use here, can play an important role in international relations research, where the threat of omitted variable bias is almost always present. Although sensitivity analysis has been applied in international relations, almost all such applications have been based on parametric regression models. In the democratic peace literature, Kadera and Mitchell conduct a parametric sensitivity analysis in the spirit of Leamer.16 In addition, Chaudoin, Hays, and Hicks apply a parametric sensitivity analysis of Altonji, Elder, and Taber to the effects of the GATT/WTO, whereas Hegre and Sambanis use the method of Sala-i-Martin to examine the sensitivity of empirical results on civil war onset.17 The only exception we found is Davis and Shirato, who use a nonparametric sensitivity analysis to assess the robustness of their findings to possible sample selection bias.18 Unlike parametric approaches, nonparametric sensitivity analyses avoid modeling assumptions and hence offer a robust method to examine the strength of empirical conclusions.

### AT: !/D – Collective Action

#### Best studies prove short-termism, truth decay, and weak multilateralism are NOT inherent to democracy, but to backsliding – and democracy’s net better at overcoming collective action problems

Lindvall 21 Daniel Lindvall, researcher at the Climate Change Leadership Initiative at the Department of Earth Sciences in Uppsala University, PhD sociology, “Democracy and the Challenge of Climate Change,” International IDEA Discussion Paper 3/2021, International Institute for Democracy and Electoral Assistance, 2021, <https://www.idea.int/sites/default/files/publications/democracy-and-the-challenge-of-the-climate-change.pdf> /GoGreen!

Although democracies do better on average than authoritarian systems, climate change is an issue that poses specific challenges to the governing capacity of democracy. The challenge of climate change is complex and has sometimes been described as a ‘wicked problem’. It is an issue in the interface between natural and human systems, and therefore it affects all spheres of life, but in unpredictable ways. The complexity of climate change is one of the prime reasons why democracies have failed to deal adequately with the crisis. The climate crisis is moreover a global challenge, and democracies have not sufficiently managed to act beyond the constraints of the national states. The short-term focus of most democratic decision-making has been an additional weakness. Democracy is a system limited by time and space, while the problem of climate change runs across generations and national borders. Moreover, the influence of fossil fuel lobbyism, corruption, policy capture and weak institutional capacity have hampered democracies from acting responsibly.

As this paper demonstrates, democracies nevertheless possess several advantages when it comes to tackling the climate crisis. Governing systems that allow civil participation, a free flow of information and processes of assessment and evaluation seem to be more capable than authoritarian regimes in dealing with issues of great complexity. Studies on climate change cooperation have also shown that, in general, democracies are more active in international negotiations and more likely to keep their political commitments. The international cooperation on climate change relies to a great extent on open and democratic societies, providing a base for journalists and civil society organizations covering and reporting on the negotiations and monitoring compliance. Moreover, technological innovation, particularly on renewable energy, has made the solutions to the climate crisis less cross-border intensive and extensive, motivating both individual countries, regions and cities, and companies, communities and individuals, to act on their own. Active engagement by individuals and civil society organizations can create pressure for strong policy responses on a local, national and global level.

Studies also show that democracies are improving their performance on long-term policies—for instance, on climate action and on the United Nations Sustainable Development Goals. Institutional changes, such as the adoption of climate legislation and advisory bodies, and activities within democracies, such as the youth-driven climate movement and processes of climate litigation, have made them even less vulnerable to short-termism. Despite this, democracies are still not delivering on their climate pledges. In many fragile democracies, corruption is obstructing the policymaking process on climate and preventing adequate and efficient implementation. The fossil fuel industry still wields substantial influence on politics in several democratic countries. In this respect, the lack of trustworthy and independent public institutions, with the ability to counteract policy capture and corruption, protect human rights, and deliver on the principles of the rule of law and good governance, is a serious barrier on the path towards a sustainable future.

In conclusion, functioning democracy is essential to effectively deal with the climate crisis; however, as long as many democracies are suffering from their own institutional failures, they will not be able deliver adequately. Consequently, efforts to develop and support democracy around the world need to be sustained, but it is also necessary to undertake certain measures, activities and reforms to make democracy more able to tackle the climate crisis. The policy advice in this paper focuses on the necessity to overcome short-termism, ensure citizen participation, act on climate injustice, develop knowledge-based decision-making and strengthen the state capacity. Further research on the nexus of democracy and climate is also needed, to better understand both the effects climate change could have on democracy as such and how democratic governance could be developed to become more capable of dealing with the crisis at hand.

### AT: US Thumps

#### It only demonstrated the resilience of democracy, does NOT thump

Walsh 21 Nate Walsh, Emmy award-winning CNN International Security Editor, “America was lucky to be saved by its democracy -- even if some don't realize it,” CNN, 1-8-2021, <https://www.cnn.com/2021/01/08/opinions/america-saved-by-democracy-paton-walsh/index.html> /GoGreen!

Even in the aftermath, America might not see how fortunate it is.

Most "attempted coups" elsewhere in the world leave a hangover of giddying uncertainty - shops shuttered, presidents in hiding, the television playing a nature documentary or half the staff in the hotel you are staying in not turning up for work.

However, America's extraordinary privileges of law and functionality seemed to sustain, even in a brief moment of collapse. Wednesday was a six-hour catastrophic policing failure, one that finally served up an image of what the souring of democracy can look like, after years of appeasement and detachment by ordinary voters.

Yet still America woke up to relative order. The system had overnight thrived persistently - news networks broadcasting and dissecting the events, with variety and transparency, and the wheels of vote certification turning, as expected. Americans perhaps also took that for granted: that they turned on the TV to hear criticism of their president, that the police and national guard swooped in to enforce the law, that outrage - not fear at the new unknown - dominated. Chaos normally follows disorder, but in the United States the cogs kept whirring.

It's been easy to say the US version of democracy was irreparably damaged by Wednesday, January 6. But, once Moscow, Beijing and Tehran have finished gloating briefly, remember too the signals that the day sent about its resilience. Yes, the United States witnessed a mob of mostly White men breaking into its Congress, because they felt the law was theirs alone, and because so many ordinary Americans spent four years thinking the horror was either too ridiculous to fear, or would just pass. But in the end, the quieter majority, not the loudest voice, remained standing. This short moment of ugly collapse should not lead Americans to dismiss the extraordinary eloquence and value of their system.

The rioters abused the privileges of their wealthy democracy - their free lives, in the richest nation on earth - to indulge in a fantastical, parallel reality, and livestream on open social media their breaking into the seat of government. It was a spoilt child version of America - so "free" to do whatever it wants, it ignored the truths, laws and decency that actually enabled that freedom. Elsewhere globally, scenes like these normally follow actual tyranny and absurd vote-rigging, palpable repression and torture - not fictional complaints that have had their (multiple) days in court.

Wednesday's violence didn't really fit the conventional description of an "attempted coup" - normally a word evoked when the military or security forces help change who's in power. "Coup" became part of the day's hurried lexicon perhaps as what was happening was so alien and unimaginable - in a capital city so absorbed with the infallibility of its processes, that it didn't really have the vocabulary for this violence. But the less-privileged former Soviet Union - where even slight gasps of freedom have been very hard won - can offer comparisons as plentifully as Eskimos are said to have words for snow.

This wasn't a "colored revolution" - like the "Orange" one in Ukraine in 2004, where hundreds of thousands of patient protestors stood in the cold for months to successfully reverse a blatantly fraudulent election. It wasn't the "Tulip" one of Kyrgyzstan in 2005, when protesters - some on horseback, also angry at a patently rigged vote - fought their way into the presidential administration, drank its liquor, rode on its exercise bikes, all while armed security forces were unwilling to open fire.

It was uglier. It reminded me most of Ukraine in 2014, when an organized group of pro-Russian protesters forced their way into the local administrations of Donetsk and Slovyansk. The "Q-Shaman" would have fit right in that mob too. These brief, drunken moments of violence and shouting were the sparks that ignited a civil war which killed thousands. The media was also attacked then by the crowd, fired up by incendiary broadcasting from Russian state-media available in the east of the Ukraine. Crimea had earlier been invaded. It was a clockwork plan for occupation by Moscow.

But when you woke up each morning in Donetsk, the system continued to fall apart. In Washington DC, the opposite was true. The system is busying itself with rectifying the problem. The extraordinary privileges Americans live with daily - and that perversely led a handful to think the armed invasion of Capitol Hill was OK - were still there.

The United States' allies and enemies will globally chew on this moment - for signs that it foments China's rise, or gives Putin another decade in power, or makes Maduro seem comparatively competent. Yet remember, between horror at what a sense of privilege among a small mob can do, there is also a moment of hope. Values worked. Unlike elsewhere in the past decades, the departing President's supporters did not take over parliament and change the government. The army did not switch sides. The rightful winner of the last election is not in hiding - he broadcast a speech, and will be president in several days. Two members of the slavishly loyal cabinet resigned.

Trump has done damage to democracy's reputation globally in ways I never imagined I would see. President-elect Joe Biden is right to say it is "fragile." It is also precious, and effective. For now, it worked. Trump and the domestic terrorism he fomented were - in this moment - defeated. There turned out to be enduring values at the heart of even some of the most compromised American elected officials. That is not a global norm.

Now is not a time for chest-thumping over American values that have slowly deteriorated for years to get to this point. But it should also not lead a country to be so spoiled in its own privileged system that it dismisses its extraordinary merits altogether. Democracy didn't fail the United States, it pretty much saved it.

The singular reason the US system has advantages over its authoritarian rivals is that it is based on the open competition and truth of ideas. The morning after this failed coup, the United States didn't wake up to a nature documentary on state TV, or find half the hotel staff missing, but was alive with a renewed vigor of self-criticism in rolling news coverage.

They should be mindful of how they might appear to those who woke up that morning in actual tyrannies: Many perhaps taking for granted how lucky they are to live in a nation where such a staggering abuse of democracy can still be eclipsed by its virtues.

## !—TERRORISM

### A/O – Terror !

#### AM&E’s key to global counterterror – and reverse causal

Walther-Puri 21 Andrea Walther-Puri, PhD candidate, Fletcher School of Law and Diplomacy, research focuses on the effects of U.S. military counterterrorism programs on longer-term security governance transformation in the Sahel, “Afghanistan: A Tragic Lesson of the US Military’s Flawed Approach to Capacity Building,” Just Security, 9-6-2021, <https://www.justsecurity.org/78086/afghanistan-a-tragic-lesson-of-the-us-militarys-flawed-approach-to-capacity-building/> /GoGreen!

In the wake of Kabul’s collapse, experts and government officials need to answer a pivotal question: why did the United States fail to build a more effective Afghan military? In its misguided focus on training and equipping, the United States failed to prioritize a results-based approach. To avoid a similar fate with other counterterrorism training missions, the United States needs to invest in and empower assessment, monitoring, and evaluation.

Since 2001, as part of U.S. counterterrorism planning in Afghanistan, successive American administrations have prioritized building the Afghan National Security Forces (ANSF) to take over the counterterrorism mission and facilitate a measured withdrawal of American forces. But the U.S. military’s approach was flawed from the start. The United States never conducted an assessment to determine the type of military Afghanistan needed given its human capital, geography, and adversary. Its approach failed to identify clear metrics for building such a force, establish a systematic monitoring and evaluation mechanism, and adequately analyze how Afghan security forces would hold up in direct action against Taliban fighters. These gaps in analysis were laid bare when Afghan security forces completely fell apart in the face of Taliban fighters, only four months after President Joe Biden announced the U.S. withdrawal.

Twenty years later, despite the United States’ $83 billion investment in the ANSF, security in Afghanistan has progressively worsened: the Taliban controls more territory than at any point in the war, the number of effective enemy-initiated attacks has steadily increased, and fear for personal safety among Afghans has never been higher.

The United States dedicated a significant amount of money, time, and attention to implementing training and equipping units, while less than one percent went to collecting the most valuable information – how the effectiveness of soldier and unit performance changed as a result of the training.

Mission Failure: The Reconstitution of the ANSF

Capacity building is extremely challenging in conflict zones where staff turn over rapidly, no single U.S. agency is in the lead, and chronic insecurity makes measuring success difficult. Afghanistan presented the added difficulty of conducting capacity building during active combat while dealing with the challenges of coordinating the efforts of an international coalition. Persistent insecurity severely undermined reconstruction efforts, forcing the United States and NATO to continuously substitute for the capacity and capability of the ANSF, which often detracted from the capacity building mission as well as the accompanying efforts to monitor and evaluate it.

There were many flaws in the way the United States measured the effectiveness of its efforts. While the U.S. Defense Department (DOD) is required by law to conduct assessment, monitoring, and evaluation of its capacity building programs, whether this is carried out and the quality of those efforts is not always guaranteed. Standardized methods to measure results did not exist in Afghanistan. During the 20-year effort, operational assessments from top U.S. military leaders exhibited entrenched optimism, which “bore no resemblance” to conditions on the ground.

In seeking to evaluate the ANSF, DOD changed assessment methodologies at least four times, resulting in varied, often contradictory conclusions about the quality and readiness of the forces. As a result, reporting tended to elevate good news and success stories over data suggesting a lack of progress. Criticism of the various assessment mechanisms included: a paucity of personnel able to execute the assessments and verify reported data, poor quality of the data collected, and improper metrics that assessed program progress (dollars spent, equipment provided, soldiers trained) rather than longer-term effects (battlefield performance, leadership, corruption).

The Writing on the Wall

In 2008, Congress created the Special Inspector General for Afghanistan Reconstruction (SIGAR) to provide quarterly reports to Congress and ensure independent oversight over the entirety of U.S. reconstruction efforts. In late 2014, at the urging of former military and civilian leadership serving in Afghanistan, SIGAR began publishing lessons learned reports to capture the progress and challenges.

SIGAR reports repeatedly expressed skepticism of the ANSF’s capacity to provide its own security and maintain facilities and equipment provided by DOD. In March 2014, General Joseph Dunford presciently warned the Senate Armed Services Committee that if the coalition troop withdrew at the end of the year, the “[Afghan security forces] will begin to deteriorate. The security environment will begin to deteriorate, and I think the only debate is the pace of that deterioration.” In 2018, then-Afghan President Ashraf Ghani estimated his army would not last six months without American “support” and “capabilities.” In its most recent assessment in March 2021, SIGAR concluded that the ANSF could neither protect the population from insurgents in large parts of the country, nor could it maintain equipment, manage supply chains, or train new soldiers, pilots, and policemen; the ANSF was “nowhere near” achieving self-sufficiency.

Beyond Afghanistan

This broken process didn’t manifest just in Afghanistan – it persists across U.S. counterterrorism programs globally. In Iraq, fewer than 1,000 fighters of the Islamic State of Iraq and Syria (ISIS) launched a surprise attack on Mosul in 2014. In response, four of 14 Iraqi army divisions – military forces that the United States spent years training, arming, and equipping – rapidly crumbled. Approximately 30,000 soldiers dropped their weapons, shed their uniforms for civilian clothes, and blended in with the fleeing masses. No one predicted that Iraqi security forces would disintegrate when facing a few thousand militants.

In addition to major counterterrorism capacity building efforts in Afghanistan and Iraq, the United States is involved in training and equipping programs in approximately 80 countries throughout Africa, Asia, and the Middle East. Based on my interviews and forthcoming research experience, in each of these cases, the U.S. government is not making results-based decisions on training mission effectiveness.

There is also a growing body of academic research that links military assistance to increased terrorist activity. The provision of military assistance has been associated in some cases with increases in terrorist attacks, fatalities and casualties, and support for terrorist groups, as well as longer terrorist campaigns and disincentivizing partner countries from disarming terrorist groups.

Mali, for example, has received significant U.S. military counterterrorism assistance since 9/11, yet Malian security forces collapsed when faced with a terrorist and separatist onslaught in 2012. Shortly thereafter, the military launched a coup that displaced the democratically elected government. Since then, two more coups have occurred, each led by the former U.S.-trained commander of Mali’s counterterrorism unit, Assimi Goita, who has since become the nation’s president.

Adaptation Drives Effectiveness

In each of these cases, the United States has failed to leverage existing assessment, monitoring, and evaluation (AM&E) practices to better understand both intended and unintended consequences. The U.S. military lacks process and prioritization for measuring capacity building effectiveness. Using the military decision-making process to plan and execute, the DOD tends to view its mission as linear and finite. By contrast, the U.S. Agency for International Development (USAID) manages programs that are cyclical and ongoing. To ensure efficacy, USAID’s program cycle seeks to plan, deliver, assess, and adapt its assistance. The critical difference is in the final step: DOD focuses on executing the order, while USAID incorporates the results of its AM&E to improve program efficacy.

Congress took a monumental step forward in reforming how DOD conducts and manages its security cooperation efforts in the enacted FY2017 National Defense and Authorization Act (NDAA). The NDAA dramatically increased congressional oversight by mandating the assessment, monitoring and evaluation of security capacity building programs. Because of DOD’s lengthy planning process, however, tangible changes will not be realized for several years.

The FY2017 NDAA also included a crucial development: the creation of an in-house AM&E workforce at DOD. The Defense Security Cooperation University was founded in September 2019, to uphold a common knowledge base across the workforce, mandate common professional standards through a required multi-tier certificate program, and prioritize continued intellectual development. To further bolster this in-house AM&E workforce and minimize dependence on third-party contractors, the NDAA mandated the establishment of teams dedicated to AM&E within the Office of the Deputy Assistant Secretary of Defense for Security Cooperation, the Defense Security Cooperation Agency, and within each Geographic Combatant Command.

Investing in Results

To build another country’s capacity to counter terrorism, the United States must improve its own competence to assess, monitor, and evaluate training programs. DOD should further invest in three crucial areas.

First, DOD needs a culture that empowers its workforce to go beyond reporting. Promotions should be contingent upon leveraging AM&E to improve program performance, rather than upon who manages the most expensive programs. The change toward results-based learning needs to cascade from the top down – specifically, the Deputy Assistant Secretary of Defense for Security Cooperation should be appropriately staffed and resourced to ensure programs institute and empower DOD’s AM&E requirements. The agency-wide perception that program evaluation is used as a punitive tool leading to budget cuts or other adverse repercussions needs to shift – no evaluation finding should be viewed as negative, but rather should be viewed as guidance for course correction.

Second, DOD needs to prioritize rigorous program design. DOD should place emphasis on a thorough upfront assessment, during which program planners analyze the situation on the ground and assess a partner nation’s needs. If these components are properly captured, the program will identify more realistic goals and have a better, smarter design. In addition, DOD has faced criticism for not prioritizing impact evaluation. Measuring program outcomes is critical to identifying whether a given program has achieved its desired effects. By identifying successful programs, DOD can focus on adapting, replicating, and testing those programs elsewhere.

Third, DOD needs a robust yet flexible feedback loop for its programs. Leadership needs to underscore the importance of iterative learning; however, the current 5-year planning cycle and congressional notification system do not afford required flexibility. In late 2021, planning is in full swing for FY2023 programs. Once in motion, the system does not allow for change even though a lot can happen in three years that could warrant adjustment. Furthermore, while DOD should continue investing in independent research on how to improve assessment, monitoring, and evaluation of security cooperation and capacity building programs, it should also incorporate findings from the growing field of academic research in this area that already exists.

Without a fundamental shift towards accountability, other recipients of U.S. military assistance stand to suffer Afghanistan’s fate. We should always have an answer to the question: “What did we accomplish?”

#### Extinction

Hayes 18 Peter Hayes, Executive Director of the Nautilus Institute for Security and Sustainability, PhD energy and resources, University of California, Berkley, "Non-State Terrorism And Inadvertent Nuclear War," Nautilus Institute for Security and Sustainability, 1-18-2018, <https://nautilus.org/napsnet/napsnet-special-reports/non-state-terrorism-and-inadvertent-nuclear-war/> /GoGreen!

Catalytic nuclear attack Catalytic nuclear attack is a metaphor for the possible malevolent third party who sets out to induce a nuclear war between two other nuclear weapons states. It is based on a metaphor drawn from chemistry whereby a catalyst increases the rate of chemical reaction without catalyst itself being destroyed. Tiny amounts of a catalyst often suffice to bring about such a transformative effect. Such a “catalytic” nuclear attack between nuclear weapons states was a serious policy concern in the nineteen-fifties in the United States where strategists were seized of the notion that a “small” nuclear weapons state (for which read “China”) could start a nuclear war between the United States and the former Soviet Union (FSU). As articulated by the ubiquitous Herman Kahn, the concern was that the small “catalytic” state instigating the conflict would be the least damaged at the end of a nuclear war, and could increase its relative power by starting a war between other nuclear armed states that resulted in their catastrophic destruction. In his classic essay outlining this argument, Donald Kobe derived what he termed to be suspicion, retaliation, destruction, catalytic war utility, and casualty matrices for each country that defined outcomes for each state in a “catalytic nuclear war.”[2] As China began to test its own nuclear weapons and the United States and the FSU began to anticipate its deployment in the sixties, the ability of the two nuclear superpowers, even at this relatively early stage in their rapidly growing nuclear forces, to overwhelmingly retaliate and damage the catalytic state soon allayed this concern. Nonetheless, the concept motivated these two nuclear armed states to strive for nuclear non-proliferation, in part driven by their mutual fear of state-sponsored nuclear terrorism should nuclear weapons and nuclear weapons technology and materials become freely available—a concern that persisted over the subsequent decades.[3] Is catalytic nuclear terrorism still a serious policy concern? Today, the notion of “catalytic” nuclear war seems archaic in certain respects, and reflected a dismissive view at the time in the United States of the rationality of a state leadership armed with nuclear weapons and facing an overwhelming external adversary—in the case of China, not just one, but soon to be two external nuclear enemies that targeted its cities and nuclear forces. As China’s minimum deterrent posture evolved, and as its nuclear threat rhetoric subsided with the end of the Cultural Revolution, so the fear of catalytic nuclear war also receded. However, the fear of a catalytic nuclear war returned with a vengeance at the end of the Cold War when multiple states found themselves nuclear-armed almost overnight due to the collapse of the former Soviet Union, or proliferated independent nuclear forces in rapid succession in South Asia and in slow motion, North Korea. In the United States and Russia, formal and informal discussion of the importance of avoiding war and nuclear war due to third party nuclear attack, by state or non-state actors, took place in diplomatic, military, and private channels, driven in part by the risk of nuclear “mega-terrorism” as the efforts of various insurgencies and global terrorist networks to acquire and use nuclear weapons came to light. The continued salience of the concept of catalytic nuclear war rests on three nested arguments. The first is that inadvertent nuclear war is possible, that is, the probability is greater than zero albeit unknowable. Multiple “threshold” events that could trigger inadvertent nuclear war are conceivable. In some unknowable combination, such drivers contribute to a probability greater than zero that nuclear war between states will occur, variously estimated at 0.1-1 percent year by strategic analysts—although there is no objective basis for such estimates, simply subjective estimates buttressed by the perception that specific near-nuclear wars punctuated the Cold War and post-Cold War decades, at which time the probability was perceived to be much higher for months at a time. The second is that of all the drivers of inadvertent war, state-supported and non-state nuclear terrorism may be the least “directly controllable” by nuclear weapons states. Moreover, such nuclear terrorist attacks may coincide in the future with the influence of other drivers that could trigger rapid escalation to nuclear first use in conditions of complex nuclear confrontation involving two or more nuclear weapons states. Thus, the non-state terrorist driver of nuclear war may render “normal” positive and negative controls on nuclear use far less stabilizing than in the past when states were the sole concern in nuclear confrontations, depending on how a terrorist nuclear attack might affect the various contributing pathways to inadvertent nuclear war (listed in the next section). The third is that such nuclear terrorist attacks may take many forms, as shown in Figure 1. Figure 1: Types of Nuclear Terrorism from Least to Most Damaging • Credible Threats of Nuclear Terrorism • Hostage Taking • Steal, Smuggle, Acquire Radioactive Material for Dirty Bomb • Steal, Smuggle, Acquire Footloose Fissile Material • Attack Reactors • Attack Spent Fuel • Simultaneous Cyber Attacks Disable Critical Infrastructure Leading to Mass Casualties or to Enable Nuclear Terrorism • Acquire Nuclear Weapon; Detonate Nuclear Weapon Notes to Figure 1: a credible threat not accompanied by one or more actions to realize the threat is the least damage act of terrorism, and rests on the perception of those threatened as to the perpetrator’s intention and capability. Many nuclear terrorism threats are made. Relatively few are credible. The types below “mere” threats are characterized by actions which may (or may not) have been preceded by credible threats. “Footloose” here is shorthand for loss of control of legitimate and authorized control entity, public or private, that is subject to diversion and seizure by a non-state entity. Cyber attacks may be part of the types of nuclear terrorism because a competent terrorist entity will employ cyberattacks as part of a nuclear terrorist attack. However, a cyber attack that disables critical infrastructure at the same time as another type of direct nuclear terrorist attack is conducted would be highly damaging and if it results of itself in mass casualties, may enable and amplify the consequences of dirty bomb or an actual nuclear detonation. In this sense, a cyber attack may be a cyber-multiplier for other types of nuclear terrorism. Of course, a cyber attack aimed at mass casualties and terrorist effects may be undertaken without any form of nuclear terrorism associated with it. Finally, acquisition of radioactive materials or fissile material may occur via theft, purchase, or self-manufacture (the least likely and most difficult of the three acquisition pathways). Some may argue that radiological weapons (dirty bombs) are not nuclear at all in that they do not involve criticality at all, just the radioactive properties of the materials, and may be relatively crude and low technology. However, some nuclear weapons aim to achieve precisely such radiological effects on varying scales and long-term radiological effects, rather than blast and other direct irradiation of targeted humans. Dirty bombs and nuclear bombs exist on a spectrum and where competent, malevolent, and motivated non-state actors might position themselves on that spectrum remains an open question. \*\*\* These many types of terrorist nuclear attack present states with starkly different potential damage, greater possible ambiguity or even opacity in terms of precursor indicators as well as identity of the perpetrator. Any of these types of attack may affect nuclear-armed states in unpredictable ways with respect to their own nuclear use decisions at times when inter-state conflict may be more or less likely. These various types of attack by non-state actors reduce into three basic categories of threat and use, as follows: Credible threat of either nuclear detonation or radiological attack with possible massive damages Actual or sub-critical nuclear detonation Actual spent fuel or reactor attack with substantial radiological release. In turn, such categories of terrorist attack might be realized in or against one or more types of targeted state, viz, a nuclear armed state, a nuclear umbrella state that receives nuclear extended deterrence from a nuclear armed state, or a non-nuclear weapons state which may or may not have nuclear fuel cycle facilities in and/or fissile material stored on its territory. (Thus, the target may or may not be a state, a state agency, or a state facility—it might be a civilian target such as a company or a religious entity; but in this paper, all terrorist nuclear attacks are assumed to take place only in places controlled by functioning states). Nuclear terrorism post-cold war: trigger for inadvertent nuclear war? The possible catalytic effect of nuclear terrorism on the risk of state-based nuclear war is not a simple linkage. The multiple types and scales of nuclear terrorism may affect state-nuclear use decisions along multiple pathways that lead to inadvertent nuclear war. These include: Early warning systems fail or are “tripped” in ways that lead to launch-on-warning Accidental nuclear detonation, including sub-critical explosions. Strategic miscalculation in crisis, show of force Decision-making failure (such as irrational, misperception, bias, degraded, group, and time-compressed decision-making) Allied or enemy choices (to seek revenge, to exploit nuclear risk, to act out of desperation) Organizational cybernetics whereby a nuclear command-control-and communications (NC3) system generates error, including the interplay of national NC3 systems in what may be termed the meta-NC3 system. Synchronous and coincident combinations of above.[4] Exactly how, where, and when nuclear terrorism may “ambush” nuclear armed states already heading for or on such a path to inadvertent nuclear war depends on who is targeting whom at a given time, either immediately due to high tension, or generally due to a structural conflict between states. Nuclear armed states today form a complex set of global threat relationships that are not distributed uniformly across the face of Earth. Rather, based on sheer firepower and reach, the nine nuclear weapons states form a global hierarchy with at least four tiers, viz: Tier 1: United States, clear technological supremacy and qualitative edge. Tier 2: Russia, China, global nuclear powers and peers with the United States due to the unique destructive power of even relatively small nuclear arsenals, combined with global reach of missile and bomber delivery systems, thereby constituting a two-tiered global “nuclear triangle” with the United States. Tier 3: France, UK, NATO nuclear sharing and delivery NATO members (Belgium, Germany, Italy, the Netherlands and Turkey) and the NATO and Pacific nuclear umbrella states (Japan, South Korea, Australia) that depend on American nuclear extended deterrence and directly and indirectly support US and US-allied nuclear operations even though they do not host nor deliver nuclear weapons themselves. Tier 4: India, Pakistan, Israel, DPRK. The first two tiers constitute the global nuclear threat triangle that exists between the United States, Russia, and China, forming a global nuclear “truel.” Each of these states targets the others; each represents an existential threat to the other; and each has a long history of mutual nuclear threat that is now a core element of their strategic identity. Tier three consists of states with their own nuclear force but integrated with that of the United States (even France!) that expand the zone of mutual nuclear threat over much of the northern and even parts of the southern hemisphere; and states that host American nuclear command, control, communications, and intelligence systems that support US nuclear operations and to whom nuclear deterrence is “extended” (if, for example, Australia’s claim to having an American nuclear umbrella is believed). The fourth tier is composed of smaller nuclear forces with a primarily regional reach and focus. Between most of these nuclear armed states and across the tiers, there are few shared “rules of the road.” The more of these states that are engaged in a specific conflict and location, the more unpredictable and unstable this global nuclear threat system becomes, with the potential for cascading and concatenating effects. Indeed, as the number of nuclear states projecting nuclear threat against each other increases, the notion of strategic stability may lose all meaning. The emergence of a fifth tier—of non-state actors with the capacity to project nuclear threat against nuclear-armed and nuclear umbrella states (although not only these states)—is a critically important possible catalytic actor in the new conditions of nuclear threat complexity that already exist today. Such a layer represents an “edge of chaos” where the attempts by nuclear armed states to exert absolute “vertical” control over the use of nuclear weapons confront the potential of non-state entities and even individuals (insiders) to engage in “horizontal” nuclear terrorism, presenting radically different control imperatives to the standard paradigm of organizational procedures, technical measures, and safeguards of various kinds. This tier is like the waves and tides on a beach that quickly surrounds and then causes sand castles to collapse. In 2010, Robert Ayson reviewed the potential linkages between inter-state nuclear war and non-state terrorism. He concluded: “…[T]hese two nuclear worlds—a non-state actor nuclear attack and a catastrophic interstate nuclear exchange—are not necessarily separable. It is just possible that some sort of terrorist attack, and especially an act of nuclear terrorism, could precipitate a chain of events leading to a massive exchange of nuclear weapons between two or more of the states that possess them.”[5] How this linkage might unfold is the subject of the next sections of this essay. Are non-state actors motivated and able to attempt nuclear terrorism? A diverse set of non-state actors have engaged in terrorist activities—for which there is no simple or consensual definition. In 2011, there were more than 6,900 known extremist, terrorist and other organizations associated with guerrilla warfare, political violence, protest, organized crime and cyber-crime. Of these, about 120 terrorist and extremist groups had been blacklisted by the United Nations, the European Union and six major countries.[6] Some have argued that the technical, organizational, and funding demanded for a successful nuclear attack, especially involving nuclear weapons, exceeds the capacity of most of the non-state actors with terrorist proclivities. Unfortunately, this assertion is not true, especially at lower levels of impact as shown in Figure 1; but even at the highest levels of obtaining authentic nuclear weapons capabilities, a small number of non-state actors already exhibit the motivation and possible capacity to become nuclear-armed. Ellingsen suggests a useful distinction that nuclear terrorists may be impelled by two divergent motivations, as shown in Figure 2, creating “opportunistic” and “patient” profiles.[7] The requirements for an opportunist non-state nuclear terrorist tend towards immediate use and the search for short-term payoffs with only tactical levels of commitment; whereas the patient non-state nuclear terrorist is able and willing to sustain a long-term acquisition effort to deal a strategic blow to an adversary in a manner that could be achieved only with nuclear weapons. [FIGURE 2 OMITTED] In turn, many factors will drive how a potential nuclear terrorist non-state organization that obtains nuclear weapons or materials may seek to employ them, especially in its nuclear command-and-control orientations. Blair and Ackerman suggest that the goals, conditions, and capacity limitations that shape a possible nuclear terrorist’s posture lead logically to three types of nuclear terrorist nuclear command-and-control postures, viz: pre-determined (in which the leadership sends a fire order to a nuclear-armed subordinate and no change is entertained and no capacity to effect change is established in the field, that is, the order is fire-and-forget); assertive (in which only the central command can issue a nuclear fire order, central control is maintained at all times, with resulting demanding communications systems to support such control); and delegative (in which lower level commanders control nuclear weapons and have pre-delegated authority to use them in defined circumstances, for example, evidence of nuclear explosions combined with loss-of-connectivity with their central command).[8] An example of such delegative control system was the November 26, 2008 attack on Mumbai that used social media reporting to enable the attacking terrorists to respond to distant controller direction and to adapt to counter-terrorist attacks—a connectivity tactic that the authorities were too slow to shut down before mayhem was achieved.[9] Logically, one might expect nuclear terrorists oriented toward short-term, tactical goals to employ pre-determined nuclear command-and-control strategies in the hope that the speed of attack and minimum field communications avoids discovery and interdiction before the attack is complete; whereas nuclear terrorists oriented toward long-term, strategic goals might employ more pre-delegative command-and-control systems that would support a bargaining use and therefore a field capacity to deploy nuclear weapons or materials that can calibrate actual attack based on communications with the central leadership with the risk of interdiction through surveillance and counter-attack. These differing strategic motivations, timelines, and strategies in many respects invert those of nuclear weapons states that rely on large organizations, procedures, and technical controls, to ensure that nuclear weapons are never used without legitimate authorization; and if they are used, to minimize needless civilian casualties (at least some nuclear armed states aspire to this outcome). The repertoire of state-based practices that presents other states with credible nuclear threat and reassures them that nuclear weapons are secure and controlled is likely to be completely mismatched with the strengths and strategies of non-state nuclear terrorists that may seek to maximize civilian terror, are not always concerned about their own survival or even that of their families and communities-of-origin, and may be willing to take extraordinary risk combined with creativity to exploit the opportunities for attack presented by nuclear weapons, umbrella, and non-nuclear states, or their private adversaries. For non-state actors to succeed at complex engineering project such as acquiring a nuclear weapons or nuclear threat capacity demands substantial effort. Gary Ackerman specifies that to have a chance of succeeding, non-state actors with nuclear weapons aspirations must be able to demonstrate that they control substantial resources, have a safe haven in which to conduct research and development, have their own or procured expertise, are able to learn from failing and have the stamina and strategic commitment to do so, and manifest long-term planning and ability to make rational choices on decadal timelines. He identified five such violent non-state actors who already conducted such engineering projects (see Figure 3), and also noted the important facilitating condition of a global network of expertize and hardware. Thus, although the skill, financial, and materiel requirements of a non-state nuclear weapons project present a high bar, they are certainly reachable. [FIGURE 3 OMITTED] Along similar lines, James Forest examined the extent to which non-state actors can pose a threat of nuclear terrorism.[10] He notes that such entities face practical constraints, including expense, the obstacles to stealing many essential elements for nuclear weapons, the risk of discovery, and the difficulties of constructing and concealing such weapons. He also recognizes the strategic constraints that work against obtaining nuclear weapons, including a cost-benefit analysis, possible de-legitimation that might follow from perceived genocidal intent or use, and the primacy of political-ideological objectives over long-term projects that might lead to the group’s elimination, the availability of cheaper and more effective alternatives that would be foregone by pursuit of nuclear weapons, and the risk of failure and/or discovery before successful acquisition and use occurs. In the past, almost all—but not all—non-state terrorist groups appeared to be restrained by a combination of high practical and strategic constraints, plus their own cost-benefit analysis of the opportunity costs of pursuing nuclear weapons. However, should some or all of these constraints diminish, a rapid non-state nuclear proliferation is possible. Although only a few non-state actors such as Al Qaeda and Islamic State have exhibited such underlying stamina and organizational capacities and actually attempted to obtain nuclear weapons-related skills, hardware, and materials, the past is not prologue. An incredibly diverse set of variously motivated terrorist groups exist already, including politico-ideological, apocalyptic-millenarian, politico-religious, nationalist-separatist, ecological, and political-insurgency entities, some of which converge with criminal-military and criminal-scientist (profit based) networks; but also pyscho-pathological mass killing cults, lone wolves, and ephemeral copy-cat non-state actors. The social, economic, and deculturating conditions that generate such entities are likely to persist and even expand. In particular, rapidly growing coastal mega-cities as part of rapid global urbanization offer such actors the ability to sustain themselves as “flow gatekeepers,” possibly in alliance with global criminal networks, thereby supplanting the highland origins of many of today’s non-state violent actors with global reach.[11] Other contributing factors contributing to the supply of possible non-state actors seeking nuclear weapons include new entries such as city states in search of new security strategies, megacities creating their own transnationally active security forces, non-states with partial or complete territorial control such as Taiwan and various micro-states, failing states, provinces in dissociating, failing states that fall victim to internal chaos and the displacement effects of untrammeled globalization, and altogether failed states resulting in ungoverned spaces. To this must be added domestic terrorist entities in the advanced industrial states as they hollow out their economies due to economic globalization and restructuring, adjust to cross-border migration, and adapt to cultural and political dislocation. In short, the prognosis is for the fifth tier of non-state actors to beset the other four tiers with intense turbulence just as waves on a beach swirl around sandcastles, washing away their foundations, causing grains of sand to cascade, and eventually collapsing the whole structure. Observed non-state nuclear threats and attacks In light of the constraints faced by non-state terrorist actors in past decades, it is not surprising that the constellation of actual nuclear terrorist attacks and threats has been relatively limited during and since the end of the Cold War. As Martha Crenshaw noted in a comment on the draft of this paper: We still don’t know why terrorists (in the sense of non-state actors) have not moved into the CBRN [chemical,biological, radiological or nuclear ] domain. (Many people think biosecurity is more critical, for that matter.) Such a move would be extremely risky for the terrorist actor, even if the group possessed both capability (resources, secure space, time, patience) and motivation (willingness to expend the effort, considering opportunity costs). So far it appears that “conventional” terrorism serves their purposes well enough. Most of what we have seen is rhetoric, with some scattered and not always energetic initiatives.[12] Nonetheless, those that have occurred demonstrate unambiguously that such threats and attacks are not merely hypothetical, in spite of the limiting conditions outlined above. One survey documented eighty actual, planned attacks on nuclear facilities containing nuclear materials between 1961-2016[13] as follows: 80 attacks in 3 waves (1970s armed assaults, 1990s thefts, post-2010, breaches) High threat attacks: 32/80 attacks posed substantial, verified threat of which 44 percent involved insiders. All types of targets were found in the data set—on reactors, other nuclear facilities, military bases leading Gary Ackerman and to conclude: “Overall, empirical evidence suggests that there are sufficient cases in each of the listed categories that no type of threat can be ignored.”[14] No region was immune; no year was without such a threat or attack. Thus, there is a likely to be a coincidence of future non-state threats and attacks with inter-state nuclear-prone conflicts, as in the past, and possibly more so given the current trend in and the generative conditions for global terrorist activity that will likely pertain in the coming decades. Of these attacks, about a quarter each were ethno-nationalist, secular utopian, or unknown in motivation; and the remaining quarter were a motley mix of religious (11 percent), “other” (5 percent), personal-idiosyncratic (4 percent), single issue (2 percent) and state sponsored (1 percent) in motivation. The conclusion is unavoidable that there a non-state nuclear terrorist attack in the Northeast Asia region is possible. The following sections outline the possible situations in which nuclear terrorist attacks might be implicated as a trigger to interstate conflict, and even nuclear war. Particular attention is paid to the how nuclear command, control and communications systems may play an independent and unanticipated role in leading to inadvertent nuclear war, separate to the contributors to inadvertency normally included such as degradation of decision-making due to time and other pressures; accident; “wetware” (human failures), software or hardware failures; and misinterpretation of intended or unintended signals from an adversary. Regional pathways to interstate nuclear war At least five distinct nuclear-prone axes of conflict are evident in Northeast Asia. These are: US-DPRK conflict (including with United States, US allies Japan, South Korea and Australia; and all other UNC command allies. Many permutations possible ranging from non-violent collapse to implosion and civil war, inter-Korean war, slow humanitarian crisis. Of these implosion-civil war in the DPRK may be the most dangerous, followed closely by an altercation at the Joint Security Area at Panmunjon where US, ROK, and DPRK soldiers interact constantly. China-Taiwan conflict, whereby China may use nuclear weapons to overcome US forces operating in the West Pacific, either at sea, or based on US (Guam, Alaska) or US allied territory in the ROK, Japan, the Philippines, or Australia); or US uses nuclear weapons in response to Chinese attack on Taiwan. China-Japan conflict escalates via attacks on early warning systems, for example, underwater hydrophone systems (Ayson-Ball, 2011). China-Russia conflict, possibly in context of loss-of-control of Chinese nuclear forces in a regional conflict involving Taiwan or North Korea. Russia-US conflict, involving horizontal escalation from a head-on collision with Russian nuclear forces in Europe or the Middle East; or somehow starts at sea (mostly likely seems ASW) or over North Korea (some have cited risk of US missile defenses against North Korean attack as risking Russian immediate response). Combinations of or simultaneous eruption of the above conflicts that culminate in nuclear war are also possible. Other unanticipated nuclear-prone conflict axes (such as Russia-Japan) could also emerge with little warning. Precursors of such nuclear-laden conflicts in this region also exist that could lead states to the brink of nuclear war and demonstrate that nuclear war is all too possible between states in this region. Examples include the August 1958 Quemoy-Matsu crisis, in which the United States deployed nuclear weapons to Taiwan, and the US Air Force has only a nuclear defense strategy in place to defend Taiwan should China have escalated its shelling campaign to an actual attack; the October 1962 Cuban Missile Crisis, when a US nuclear armed missile was nearly fired from Okinawa due to a false fire order; the March 1969 Chinese-Soviet military clash and resulting consideration of nuclear attacks by both sides; and the August 1976 poplar tree crisis at Panmunjon in Korea, when the United States moved nuclear weapons back to the DMZ and the White House issued pre-delegated orders to the US commander in Korea to attack North Korea if the tree cutting task force was attacked by North Korean forces. Loss-of-control of Nuclear Weapons As is well known, nuclear armed states must routinely—and in the midst of a crisis—ensure that their nuclear weapons are never used without legitimate authority, but also ensure at the same time that they are always available for immediate use with legitimate authority. This “always-never” paradox is managed in part by a set of negative and positive controls, reliant upon procedural and technical measures, to maintain legitimate state-based command-and-control (see Figure Four). [FIGURE 4 OMITTED] In this framework, Jerry Conley has produced a taxonomy of nuclear command-and-control structures that embody varying notional national “command-and-control” orientations (also referred to as stability points or biases). Each nuclear armed state exhibits a distinct preference for technical and procedural measures to achieve negative and positive control of nuclear weapons. The way that a state constructs its control system varies depending on its size, wealth, technology, leadership, and strategic orientation, lending each state a unique use propensity affected by the information processing and transmission functions of the nuclear command-and-control system, that in part determines the use or non-use decisions made by the leaders of nuclear armed states. The resulting ideal nuclear command-and-control state structures are shown in Table 1. [TABLE 1 OMITTED] These ideal types are summarized with respect to the defining axes of control measure in Figure Five. [FIGURE 5 OMITTED] In Northeast Asia, a four-way nuclear threat system exists that has a three world-class nuclear armed states, the United States, Russia and China, interacting with a fourth tier, barely nuclear armed state, the DPRK. In this quadrilateral nuclear standoff, the DPRK’s simple NC3 system likely is an amalgam of a poorly resourced, militarized, and personalized leadership—which may lead it to oscillate between procedural and technical measures as the basis of control, with a primary emphasis on positive use control, not negative control to avoid unauthorized use. China’s large, centralized NC3 system co-mingles nuclear and conventional communications between national commanders and deployed nuclear forces and may emphasize negative more than positive use controls to ensure Party control. Russia’s highly centralized, complex NC3 system relies on legacy technology and limited economic base for modernization. It too may be more oriented towards negative controls in peacetime, but have the capacity to spring almost instantly to primary reliance on positive controls in times of crisis or tension. The US NC3 system is large, complex and based on wealth and technological prowess. It is under civilian, not military control, at least in principle and in peacetime, and is redundant, diverse, and relatively resilient. Non-state nuclear attack as trigger of inter-state nuclear war in Northeast Asia The critical issue is how a nuclear terrorist attack may “catalyze” inter-state nuclear war, especially the NC3 systems that inform and partly determine how leaders respond to nuclear threat. Current conditions in Northeast Asia suggest that multiple precursory conditions for nuclear terrorism already exist or exist in nascent form. In Japan, for example, low-level, individual, terroristic violence with nuclear materials, against nuclear facilities, is real. In all countries of the region, the risk of diversion of nuclear material is real, although the risk is likely higher due to volume and laxity of security in some countries of the region than in others. In all countries, the risk of an insider “sleeper” threat is real in security and nuclear agencies, and such insiders already operated in actual terrorist organizations. Insider corruption is also observable in nuclear fuel cycle agencies in all countries of the region. The threat of extortion to induce insider cooperation is also real in all countries. The possibility of a cult attempting to build and buy nuclear weapons is real and has already occurred in the region.[15] Cyber-terrorism against nuclear reactors is real and such attacks have already taken place in South Korea (although it remains difficult to attribute the source of the attacks with certainty). The stand-off ballistic and drone threat to nuclear weapons and fuel cycle facilities is real in the region, including from non-state actors, some of whom have already adopted and used such technology almost instantly from when it becomes accessible (for example, drones).[16] Two other broad risk factors are also present in the region. The social and political conditions for extreme ethnic and xenophobic nationalism are emerging in China, Korea, Japan, and Russia. Although there has been no risk of attack on or loss of control over nuclear weapons since their removal from Japan in 1972 and from South Korea in 1991, this risk continues to exist in North Korea, China, and Russia, and to the extent that they are deployed on aircraft and ships of these and other nuclear weapons states (including submarines) deployed in the region’s high seas, also outside their territorial borders. The most conducive circumstance for catalysis to occur due to a nuclear terrorist attack might involve the following nexi of timing and conditions: Low-level, tactical, or random individual terrorist attacks for whatever reasons, even assassination of national leaders, up to and including dirty radiological bomb attacks, that overlap with inter-state crisis dynamics in ways that affect state decisions to threaten with or to use nuclear weapons. This might be undertaken by an opportunist nuclear terrorist entity in search of rapid and high political impact. Attacks on major national or international events in each country to maximize terror and to de-legitimate national leaders and whole governments. In Japan, for example, more than ten heads of state and senior ministerial international meetings are held each year. For the strategic nuclear terrorist, patiently acquiring higher level nuclear threat capabilities for such attacks and then staging them to maximum effect could accrue strategic gains. Attacks or threatened attacks, including deception and disguised attacks, will have maximum leverage when nuclear-armed states are near or on the brink of war or during a national crisis (such as Fukushima), when intelligence agencies, national leaders, facility operators, surveillance and policing agencies, and first responders are already maximally committed and over-extended. At this point, we note an important caveat to the original concept of catalytic nuclear war as it might pertain to nuclear terrorist threats or attacks. Although an attack might be disguised so that it is attributed to a nuclear-armed state, or a ruse might be undertaken to threaten such attacks by deception, in reality a catalytic strike by a nuclear weapons state in conditions of mutual vulnerability to nuclear retaliation for such a strike from other nuclear armed states would be highly irrational. Accordingly, the effect of nuclear terrorism involving a nuclear detonation or major radiological release may not of itself be catalytic of nuclear war—at least not intentionally–because it will not lead directly to the destruction of a targeted nuclear-armed state. Rather, it may be catalytic of non-nuclear war between states, especially if the non-state actor turns out to be aligned with or sponsored by a state (in many Japanese minds, the natural candidate for the perpetrator of such an attack is the pro-North Korean General Association of Korean Residents, often called Chosen Soren, which represents many of the otherwise stateless Koreans who were born and live in Japan) and a further sequence of coincident events is necessary to drive escalation to the point of nuclear first use by a state. Also, the catalyst—the non-state actor–is almost assured of discovery and destruction either during the attack itself (if it takes the form of a nuclear suicide attack then self-immolation is assured) or as a result of a search-and-destroy campaign from the targeted state (unless the targeted government is annihilated by the initial terrorist nuclear attack). It follows that the effects of a non-state nuclear attack may be characterized better as a trigger effect, bringing about a cascade of nuclear use decisions within NC3 systems that shift each state increasingly away from nuclear non-use and increasingly towards nuclear use by releasing negative controls and enhancing positive controls in multiple action-reaction escalation spirals (depending on how many nuclear armed states are party to an inter-state conflict that is already underway at the time of the non-state nuclear attack); and/or by inducing concatenating nuclear attacks across geographically proximate nuclear weapons forces of states already caught in the crossfire of nuclear threat or attacks of their own making before a nuclear terrorist attack.[17] An example of a cascading effect would be a non-state attack on a key node of linked early warning systems that is unique to and critical for strategic nuclear forces to be employable, or the effect of multiple, coincident and erroneous sensor alerts of incoming attacks (as occurred during the Cuban Missile Crisis with radar in Florida monitoring Soviet missiles in Cuba that mistakenly fused an erroneous reading of a missile trajectory with a real observation of a Soviet satellite that happened to be passing overhead). An example of a concatenating effect would an attack that leads a nuclear weapons state to target two other states forces because it cannot determine whose forces attacked its own. This circumstance might arise if key anti-submarine forces or an aircraft carrier battle group were attacked and it was impossible to determine in a given waterway or area of ocean whose submarines were present or responsible for the attack, leading the attacked state to destroy all the submarines presenting on-going threat to its strategic forces. As we noted above, a terrorist nuclear shock may take various forms and appear in different places. Ever since an extortion attempt in Boston in 1974 based on the threat of nuclear detonation, the threat of an improvised nuclear device has been credible. For such a threat to be credible, a non-state terrorist entity must release a plausible precursor such as nuclear material or warhead design information, or stage an actual demonstration attack that makes it plausible that the attacker controls a significant quantity of fissile material (most likely plutonium, or simply radioactive materials suitable for a radiological device that might be used to draw in first responders and then detonate a warhead to maximize damage and terror). Such an attack might be combined with a separate attack on critical infrastructure such as a cyberattack. The attacker might retain sufficient material for bargaining and insurance should the initial attack fail. Given the need to adapt to circumstances, such an attacker is likely to be patient and strategic, in the terms defined earlier, and to have extensive organizational and communication capacities; and to be able to operate at multiple targeted sites, possibly in multiple countries. Given its patience and stamina, such an attacker would select a highly symbolic target such as a high level meeting. Such a case would present the targeted state with an exquisite dilemma: bargaining and negotiation with the non-state actor threatening such an attack may be justified given the explicit and plausible nature of the threat, which may be politically impossible while making counter-terrorism operations very risky and only possible with extreme caution. And, such an attacker might well issue a false statement about state-sponsorship to invoke third parties in ways that vastly complicate the response to the threat. If the attacker is less capable and driven for immediate political or other returns, then it may be satisfied with highly delegated delivery with no recall option, and no use of communications to minimize the risk of discovery or interdiction. Such an attacker is also less likely to wait for the circumstances in which inter-state nuclear war is more likely due to inter-state tension; and also less likely to seek third party effects beyond the damage to the immediate target and resulting terror. Should surveillance indicate that an improvised nuclear device is in motion, then an all-out search to interdict the attackers and to retrieve the device or materials would likely ensue. In these two instances of credible threat of non-state nuclear attack, the insider versus outsider perpetrator factor will affect significantly how the attack affects possible inter-state conflicts. In Kobe’s terms, if the perpetrator is confirmed to be an outsider, then a country-of-origin suspicion matrix may cast suspicion onto another state as possible sponsor. For an attack threatened in China, the linkage might be back to Russia, the United States, or North Korea. For an attack threatened in Russia, the linkage might be back to the United States, China, or North Korea. For an attack threatened in North Korea, the linkage might be back to the United States, China, or Russia. And for an attack threatened in one of the umbrella states in the region, South Korea and Japan, such an attack might be linked to each other, as well as to China, North Korea, or Russia. In each case, the shadow of suspicion and possible accusations could tilt decision-making processes in one or more of these states and ways that could worsen pre-existing views about the nuclear use propensity of an opposing nuclear armed state. Should an actual nuclear attack occur, the situation is even more complex and problematic. Such an attack might be purely accidental, due to hardware, software, or human error while nuclear materials or weapons are in transit. In principle, this limits the site of such an event to the nuclear weapons states or their ships and aircraft as neither South Korea nor Japan host nuclear weapons today. If an insider is involved, then the perpetrator may be identified quickly, and whether there is a linkage with another state may become evident (depending on nuclear forensics as well as insight obtained from surviving attackers). If an outsider is the perpetrator, then the suspicion matrix will come into play again, with possibly severe effects on inter-state tension due to accusation, suspicion, and fear of follow-on attacks. During the attack, especially if it is a hostage-taking type of attack, the identity of the perpetrator may be unknown or ambiguous, and maintaining this ambiguity or even opacity as to the attacker may be deliberate—as was the case with the 2008 Mumbai attack in which the controller tried to ensure that all the attackers were killed in the course of the twelve separate but coordinated attacks across the city over four days. Although much progress has been made in establishing local nuclear forensics capability in Japan,[18] China, and South Korea, there is no certainty that it is sufficiently developed to identify the perpetrator of an act of nuclear terrorism, especially if there is a state sponsor and deception involved. Conclusion We now move to our conclusion. Nuclear-armed states can place themselves on the edge of nuclear war by a combination of threatening force deployments and threat rhetoric. Statements by US and North Korea’s leaders and supporting amplification by state and private media to present just such a lethal combination. Many observers have observed that the risk of war and nuclear war, in Korea and globally, have increased in the last few years—although no-one can say with authority by how much and exactly for what reasons. However, states are restrained in their actual decisions to escalate to conflict and/or nuclear war by conventional deterrence, vital national interests, and other institutional and political restraints, both domestic and international. It is not easy, in the real world, or even in fiction, to start nuclear wars.[19] Rhetorical threats are standard fare in realist and constructivist accounts of inter-state nuclear deterrence, compellence, and reassurance, and are not cause for alarm per se. States will manage the risk in each of the threat relationships with other nuclear armed states to stay back from the brink, let alone go over it, as they have in the past. This argument was powerful and to many, persuasive during the Cold War although it does not deny the hair-raising risks taken by nuclear armed states during this period. Today, the multi-polarity of nine nuclear weapons states interacting in a four-tiered nuclear threat system means that the practice of sustaining nuclear threat and preparing for nuclear war is no longer merely complicated, but is now enormously complex in ways that may exceed the capacity of some and perhaps all states to manage, even without the emergence of a fifth tier of non-state actors to add further unpredictability to how this system works in practice. The possibility that non-state actors may attack without advance warning as to the time, place, and angle of attack presents another layer of uncertainty to this complexity as to how inter-state nuclear war may break out. That is, non-state actors with nuclear weapons or threat goals and capacities do not seek the same goals, will not use the same control systems, and will use radically different organizational procedures and systems to deliver on their threats compared with nuclear armed states. If used tactically for immediate terrorist effect, a non-state nuclear terrorist could violently attack nuclear facilities, exploiting any number of vulnerabilities in fuel cycle facility security, or use actual nuclear materials and even warheads against military or civilian targets. If a persistent, strategically oriented nuclear terrorist succeed in gaining credible nuclear threat capacities, it might take hostage one or more states or cities. If such an event coincides with already high levels of tension and even military collisions between the non-nuclear forces of nuclear armed states, then a non-state nuclear terrorist attack could impel a nuclear armed state to escalate its threat or even military actions against other states, in the belief that this targeted state may have sponsored the non-state attack, or was simply the source of the attack, whatever the declared identity of the attacking non-state entity. This outcome could trigger these states to go onto one or more of the pathways to inadvertent nuclear war, especially if the terrorist attack was on a high value and high risk nuclear facility or involved the seizure and/or use of fissile material. Some experts dismiss this possibility as so remote as to be not worth worrying about. Yet the history of nuclear terrorism globally and in the Northeast Asian region suggests otherwise. Using the sand castle metaphor, once built on the high tide line, sand castles may withstand the wind but eventually succumb to the tide once it reaches the castle—at least once, usually twice a day. Also, theories of organizational and technological failure point to the coincidence of multiple, relatively insignificant driving events that interact or accumulate in ways that lead the “metasystem” to fail, even if each individual component of a system works perfectly. Thus, the potential catalytic effect of a nuclear terrorist incident is not that it would of itself lead to a sudden inter-state nuclear war; but that at a time of crisis when alert levels are already high, when control systems on nuclear forces have already shifted from primary emphasis on negative to positive control, when decision making is already stressed, when the potential for miscalculation is already high due to shows of force indicating that first-use is nigh, when rhetorical threats promising annihilation on the one hand, or collapse of morale and weakness on the other invite counter-vailing threats by nuclear adversaries or their allies to gain the upper hand in the “contest of resolve,” and when organizational cybernetics may be in play such that purposeful actions are implemented differently than intended, then a terrorist nuclear attack may shift a coincident combination of some or all of these factors to a threshold level where they collectively lead to a first-use decision by one or more nuclear-armed states. If the terrorist attack is timed or happens to coincide with high levels of inter-state tension involving nuclear-armed states, then some or all of these tendencies will likely be in play anyway—precisely the concern of those who posit pathways to inadvertent nuclear war as outlined in section 2 above. The critical question is, just as a catalyst breaks some bonds and lets other bonds form, reducing the energy cost and time taken to achieve a chemical reaction, how would a nuclear terrorist attack at time of nuclear charged inter-state tension potentially shift the way that nuclear threat is projected and perceived in a four or five-way nuclear-prone conflict, and how might it affect the potential pathways to inadvertent nuclear war in such a system? Such a pervasive incremental effect is shown in Figure 6 below. [FIGURE 6 OMITTED] Any one or indeed all of these starting nuclear control profiles may be disputed, as might the control profile at the end of the response arrow. (In Figure 6, each nuclear state responds to a terrorist nuclear attack by loosening or abandoning negative controls against unauthorized use, and shifts towards reliance mostly on positive procedural controls biased towards use). But each nuclear armed state will make its moves in response to the posited terrorist nuclear attack partly in response to its expectations as to how other nuclear armed states will perceive and respond to these moves, as well as their perception that an enemy state may have sponsored a terrorist nuclear attack—and considered together, it is obvious that they may not share a common image of the other states’ motivations and actions in this response, leading to cumulative potential for misinterpretation and rapid subsequent action, reaction, and escalation. It is also conceivable—although intuitively it would seem far less likely–that a terrorist nuclear attack at such a conjuncture of partly or fully mobilized nuclear armed states might induce one or more of them to stand down, slow down its decision making or deployments, establish new communication channels with potential nuclear enemy states, and even make common cause to hunt down and eliminate the non-state nuclear terrorist entity, or coordinate operations to respond to the threat of a second terrorist nuclear attack—the credibility of which would be high in the aftermath of a successful initial non-state nuclear attack. As Robert Ayson concluded: In considering the ways in which a terrorist nuclear attack could (wittingly or unwittingly) spark off a wider nuclear exchange government leaders are entitled to be just as worried about their own actions—how they would respond to a terrorist nuclear attack and how that response might get very catastrophically out of control—as about the terrorist act per se. If so, states need to do more than consider the best ways to prevent terrorists from acquiring, deploying and then detonating a nuclear weapon. They also need to think about how they can control themselves in the event of a nuclear terrorist attack (even if some might suggest this risks handing the terrorist a premature and unnecessary victory by giving them indirect influence over the choices states make).[20]

### AT: !/D – Nuke Terror

#### Counterterror cooperation is why cause-of-death stats don’t reflect the inevitability of nuclear terrorism – motive, means, opportunity, and organizational capacity are all growing

Allison 18 Dr. Graham Allison, Professor of Government at Harvard Kennedy School, “Nuclear Terrorism: Did We Beat the Odds or Change Them?” PRISM, 7(3), 5-15-2018, <https://cco.ndu.edu/News/Article/1507316/nuclear-terrorism-did-we-beat-the-odds-or-change-them/> /GoGreen!

Not surprisingly, the book attracted critics as well. The most common objection focused on what skeptics argued was an irresolvable contradiction between the core claims of “inevitable” and “preventable.” If something is preventable, then it cannot be inevitable, they said.

My attempt to answer their point was proving largely ineffective, since for the most part, I just kept repeating the argument stated in the book. But fortunately, I was rescued by none other than Buffett himself. In making judgments about buying stocks, and even more in owning and running several reinsurance companies, Buffett had become a legendary oddsmaker. Those businesses had also forced him to think seriously about nuclear terrorism as one of what investors call “fat tail” risks. He had concluded that such an event was virtually inevitable and that the consequences would be devastating. Thus he prohibited his companies from writing insurance against nuclear terrorism.

The following two charts clarify Buffett’s argument. Chart 1 demonstrates that if the probability of a successful nuclear terrorist attack in the year ahead is 10 percent, and if that condition persists for 50 years, the likelihood of nuclear terrorism occurring is almost 100 percent (99.5 percent to be precise).3

**[CHART 1 OMITTED]**

Chart 1: Probability of Nuclear Terrorist Attack if Annual Odds are 10 percent.

But as Chart 2 illustrates, if actions were taken to reduce that likelihood from 10 percent a year to 1 percent, the probability that in the next 50 years there is no successful nuclear terrorist incident rises from almost zero to 60.5 percent. These extrapolations are, as Buffett explains, simple probability calculations.4

**[CHART 2 OMITTED]**

Chart 2: Probability of Nuclear Terrorist Attack if Annual Odds are 1 percent.

Prior to publication, a number of referees pointed out that even if one agreed that the risks of nuclear terrorism were much greater than had been previously recognized, the policy community would ask: how likely is such an event, now? As one wag put it, what moves most Washingtonians are consequences that could happen on their watch. Even those who found Buffett’s response analytically correct argued that it was too “academic” for many participants in the policy debate.

Thus at their urging, in the final published text of Nuclear Terrorism I offered my best judgment. Specifically, I wrote that on the trajectory we were following in 2004, absent significant additional preventive actions, the likelihood that terrorists would successfully explode a nuclear bomb somewhere in the world in the decade ahead was “more likely than not.” As a leading advocate of what I call “betable propositions”—putting one’s money where one’s mouth is—I made a number of bets with colleagues who were more skeptical.5 Operationalizing my estimate, I bet $51 of my money against $49 of theirs that before December 31, 2014 we would see an act of nuclear terrorism. Needless to say, I was happy to lose these bets.

With the benefit of hindsight, it is fair to ask whether my 2004 assessment of the risk was wrong. To begin to try to answer that question, it is necessary to start with candor about the larger question of which it is a component. The cosmic question is why there has been no mega-terrorist attack on the United States since September 11, 2001 when al-Qaeda operatives crashed commercial airliners into the World Trade Center and Pentagon.

In the wake of that attack, anyone who had offered to bet that 16 years on there would have been no terrorist attack on the United States that killed more than 100 people would have been able to get 1000:1 odds. In each of the years since that attack, the annual threat assessment from the U.S. Intelligence Community (IC) has ranked terrorism as among the top three threats to the United States. Polls find that more than 80 percent of Americans expect another major terrorist attack in the near future.6 Half of Americans expect that they or a member of their family will be killed by terrorists.7

How can we square these expectations with what has actually happened? Who or what has actually killed Americans here in the United States during the decade and a half since the al-Qaeda strike on 9/11? On the record, tree limbs and other falling objects have killed 100 times more Americans than terrorist attacks. As Chart 3 demonstrates, apart from old age and disease, the leading causes of death for Americans here at home have been opioid overdoses (40,000); car accidents (39,000); and suicide (38,000).8

**[CHART 3 OMITTED]**

Chart 3: Average Annual Deaths in the United States by Method of Death.

Thus, to put it bluntly, it is hard to deny the gap between the expectations of the intelligence and policy analytic community who have been trying to understand terrorism and counterterrorism, on the one hand, and the brute facts, on the other.

In attempting to understand the challenge of terrorism, analysts have used versions of Sherlock Holmes’s framework of “MMO”—motive, means, and opportunity. Identify actors who have the motivation, means, and opportunity to commit an act of terrorism, and one has the suspect list. My modified version of Holmes includes an additional “O” for organizational capability. Individuals or groups motivated to take an action but lacking the organizational skills to use available means to exploit opportunities remain only potential risks.

Employing this MMOO framework to the challenge of terrorism since 9/11, what do we find? Potential perpetrators motivated to conduct terrorist attacks on the United States have multiplied beyond anyone’s expectation in 2001. By invading and occupying Iraq and Afghanistan, and striking targets in many other countries with drones, the United States has created new enemies. In Iraq and Afghanistan, our counterinsurgency campaigns on behalf of one faction against others have given thousands of other people motives to seek revenge against us. In what the Bush Administration labeled the “Global War On Terrorism,” U.S. forces have conducted attacks on the territory of at least seven Muslim-majority nations—killing individuals we labeled “terrorists,” but also civilians who are known as collateral damage. These actions have provided fodder that extremists have used skillfully to recruit and motivate payback. Indeed, the Osama bin Laden dream to ignite a “clash of civilizations” between Muslims and what he called the “Jewish-Christian crusaders” has more credibility today than anyone could have imagined at the beginning of the century.

While post–9/11 security measures have made it more difficult to hijack a commercial airliner, the means by which to kill double, triple, and even quadruple digit numbers of people have also expanded. As the Orlando and Las Vegas shootings suggested, in many states in the United States, it is not that hard to buy an assault rifle and ammunition that will allow a shooter to fire 1,000 rounds in two minutes. And recent truck attacks by ISIL-inspired fighters in Nice, Barcelona, and New York demonstrate that terrorists recognize that modern life offers them many means by which to carry out their attacks.9 The internet has also expanded the availability of chemicals, deadly opioids like fentanyl, and even pathogens. Web-accessible information about how to make elementary bombs or acquire and use pathogens like anthrax has also increased.

Opportunities to kill hundreds or even thousands of Americans also abound. As military planners would put it, the United States offers a “target-rich” environment. Terrorists intent on killing large numbers could find them everywhere: from malls and movie theaters to sports stadiums and churches.

Organizational capability appears to have been terrorists’ Achilles’ heel. The planner of 9/11, Khalid Sheikh Mohammed, demonstrated extraordinary imagination and operational skills. Intelligence professionals gave his design and execution of the plan an “A.” Fortunately, he has been one of the few. Advances in al-Qaeda’s bombmaking appear to be traceable also to a single individual—Ibrahim al-Asiri. He developed the bombs for the failed underwear bomb plot in 2009 and cargo hold plot in 2010, as well as the laptop bomb that led the Trump Administration to temporarily ban laptops on flights.10

Terrorists have for the most part been “technically challenged.” Should that factor change, the overall picture could also change dramatically overnight.

In sum, the question about why there has been no nuclear terrorist attack is one piece of the larger puzzle about why there has been no mega-terrorist attack of any kind. And the deeper question behind that is whether we in the analytic community have a good grasp on the fundamentals of this challenge. Truth be told, I register my doubts.

Nonetheless, I am not ready to conclude that my 2004 estimate of the odds of a nuclear terror attack was incorrect. And contrary to the claims of a number of critics, as a matter of statistics, the evidence of the past 13 years does not require me to do so. A brief aside on the logic of betting and odds will explain why. Imagine a coin that was slightly weighted so that it had a 51 percent chance of landing heads and 49 percent chance of tails. From a single toss of that coin that landed tails, what could one conclude? Statistically, the answer is—very little. Such a result would be expected to happen 49 out of every 100 times the coin was tossed. If we tossed the coin a second time, and again it landed tails, statisticians would again remind us that the chances of that occurring were 1 in 4. To conclude as a matter of statistics that my estimate was incorrect would take a lifetime of successive decades in which there was no successful nuclear attack.11 Thus, I stand behind my assessment in 2004 that the odds of an attack in the next decade were greater than even. (As we all know, dozens of planned terrorist attacks have failed or been foiled—from the Christmas Day underwear bomber to the Times Square bombers.)

The issue this article addresses is whether in the past decade we have just beaten the odds, or whether actions we have taken have changed the odds for the better. To address that question, it is necessary to review the array of factors and actions that have reduced the risk of nuclear terrorism on the one hand, and those that have increased the risk on the other.

Consider, for example, what would likely have happened after 9/11 had Osama bin Laden and al-Qaeda been able to continue operating from their headquarters in Afghanistan. As the video bin Laden made after the attack demonstrated, he was thrilled by what Khalid Sheikh Mohammed’s operation had achieved. He later called on all faithful Muslims to join the jihad and top 9/11. At the pinnacle of his pyramid of destruction was a mushroom cloud enveloping one of the great cities of the world. What prevented that first and foremost was a relentless counterterrorism campaign that killed or captured most of al-Qaeda’s leadership and left the others spending most of their time trying to survive rather than perfecting plots for future terrorist attacks. Destruction of their headquarters and training camps meant that thousands of individuals who would have been planning, training, and then conducting terrorist attacks never got their chance. On the other hand, the failure to stop North Korea from developing a nuclear arsenal, as well as the collapse of U.S.–Russian nuclear security cooperation, have created new significant risks.

Section II of this article reviews actions taken that have reduced the risk of nuclear terrorism. Section III reviews factors and actions that have increased these risks. A concluding section offers an updated assessment of the risks posed by nuclear terrorism from the perspective of year-end 2017. While applauding thousands of actions that have been taken by hundreds of thousands of individuals in the past 13 years to reduce these risks, reviewing all the pluses and all the minuses, my gut tells me that the chances of a successful nuclear terrorist attack in the decade that began in 2015—in effect, the second flip of the coin—are better than even. Specifically, I believe the odds of a successful nuclear terrorist attack somewhere in the world before the end of 2024 are 51 percent or higher. While giving thanks that terrorists have failed to achieve their deadliest ambitions, in my view that is not grounds for complacency, but rather a reason for redoubling our efforts.

I am aware that on an issue about which I am passionate, I may have slipped from analysis to advocacy. The central point is not whether the odds of a nuclear terrorist attack are 51 percent or 15 percent. Threat equals likelihood times consequences, and in this case, the consequences would be devastating. Since the costs of actions to reduce these risks are modest, prudent policymakers should focus on the feasible agenda of actions.

Factors and Actions That Have Reduced the Risk of Nuclear Terrorism

In the past decade, the United States and its international partners have taken literally thousands of specific actions that closed what had been open doors to terrorists acquiring a nuclear bomb, or nuclear materials from which they could have fashioned an improvised nuclear weapon. In terms of the MMOO framework, U.S. counterterrorism and counterproliferation actions have significantly diminished both the means and the opportunities.

On the counterterrorism front, the terrorist groups that sought to attack the United States with nuclear weapons have been decimated. Osama bin Laden, Khalid Sheikh Mohammed, and most of the operational talent behind 9/11 have been captured or killed. While Osama bin Laden’s deputy, Zawahiri, succeeded him as head of al-Qaeda, and while several of the key operatives including Abdel Aziz al Masri, who led the organization’s nuclear program, remain missing, the deadly pursuit of the entire roster of the organization by collaborative intelligence, Special Operations Forces, and drones has severely diminished al-Qaeda’s ability to mount a nuclear terrorist attack.

Al-Qaeda’s successor as the greatest terror threat to the United States, Islamic State of Iraq and the Levant (ISIL), has also suffered heavy losses in recent months. In 2014, ISIL acquired a broad swath of territory across Iraq and Syria—a safehaven in which it could train militants, plot attacks, and compile resources. While we know less about ISIL’s efforts to acquire nuclear materials, the fact that the Belgian police discovered that ISIL agents involved in the 2015 terrorist attacks had surveillance footage of a Belgian nuclear research facility is suggestive.12 Furthermore, its ideological centerpiece—an epic final battle with the West—would seem to require nuclear Armageddon. By wiping out its safehavens in Syria and Iraq, the United States and its partners have diminished ISIL’s ability to organize a major effort to acquire nuclear weapons.

## LINKS

### L – Off-Budget

#### Planners can’t handle plan’s unbudgeted, last-minute reprioritization – inflexibility and lack of coordination make disruption disproportionate

Kelly 10 Terrence K. Kelly, principal mathematician at the RAND Corporation, former director of the RAND Homeland Security Research Division, formerly served for 20 years as a commissioned officer in the U.S. Army, positions included senior national security officer in the White House Office of Science and Technology Policy, PhD mathematics, Rensselaer Polytechnic Institute; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; Cathryn Quantic Thurston, Political Scientist at RAND, PhD Conflict Analysis and Resolution, George Mason University; Jennifer D. P. Moroney, senior political scientist at RAND, PhD international relations, University of Kent at Canterbury; and Charlotte Lynch, researcher at RAND; “Security Cooperation Organizations in the Country Team Options for Success,” RAND Corporation, 2010, <https://apps.dtic.mil/sti/pdfs/ADA517323.pdf> /GoGreen!

The RAND research team found that organizations that currently manage security cooperation (Title 10 U.S.C.) and security assistance (Title 22 U.S.C.) work relatively well in most countries where peacetime engagement is the norm. Many sources refer to these organizations collectively as performing “security cooperation” and we will follow this practice, differentiating between them only when needed for clarity. In particular, if security cooperation efforts can be planned in advance and there is no need for significant changes during a given budget year, current practices and authorities suffice. However, as we detail below, there is room for improvement. When unbudgeted requirements arise during a fiscal year, whether they are new programs or significant changes to existing programs, the current system presents difficulties, due to inflexible authorities and funding mechanisms, as well as sometimes less-than-ideal interagency coordination.

### L – Emerging Tech

#### SC in emerging tech is particularly resource-intensive

Chollet 20 Derek Chollet, executive vice president and senior advisor for security and defense policy at The German Marshall Fund of the United States, former US assistant secretary of defense for international security affairs; Steven Keil, fellow at GMF; and Christopher Skaluba, director of the Transatlantic Security Initiative in the Atlantic Council’s Scowcroft Center for Strategy and Security, former principal director for European and NATO Policy in the Office of the Secretary of Defense; “Rethink and replace two percent,” NATO 20/2020, The Atlantic Council, 10-14-2020, https://www.atlanticcouncil.org/content-series/nato20-2020/rethink-and-replace-two-percent/ /GoGreen!

In an ideal world, NATO could keep discussions about burden sharing out of the public eye altogether, granting that any organization with thirty democratic members will inevitably have disparities. This would require the US public and political community to recognize what is self-evident to much of the policy community—that the benefits the United States accrues from NATO are worth the costs.

To be clear, NATO’s effectiveness requires capable militaries, and this will be expensive. Tough decisions will always be required. Real work needs to be done to expand defense investment in equipment, readiness, emerging technologies, digitalization, and research and development. Substantial and targeted spending to create effective deterrence, particularly by large European countries like Germany, must remain a priority. We need to do all this in a way that avoids the pitfalls of oversimplification and acrimony that have too often defined the two-percent debate over the last decade.

The point of two percent was to get Europe to do more. That is happening. Now the discussion must move forward in a different way, and 2021 is the time to start.

#### Unique legal, policy, and security requirements are perceived as a bottomless pit of time, money AND scarce STEM experts

--AFRL = United States Air Force Research Laboratory

Cellante 21 Tony Cellante, MA candidate, International Affairs – Technology, Management, Columbia University, MBA NYU Stern School of Business, BS Management, Binghampton University; and Andreina Ray, MA candidate, International Affairs, Columbia University, MBA candidate, Columbia Business School, BA International Relations and Affairs, American University; “Advancing American Defense Technology Leadership through AFRL’s International Partnership Network,” Columbia University School of International and Public Affairs, 12-13-2021, <https://www.sipa.columbia.edu/file/15525/download?token=1CXyyxeA> /GoGreen!

Legal, Policy, Security

AFRL faces many legal, policy, and security challenges when establishing technology collaborations with international partners. Navigating this bureaucracy is time consuming and can be highly resource intensive depending on the modality of the partnership and the nature of the partner. As such, the speed and level of effort required to establish a partnership can serve as an impediment or disincentive. Another challenge stems from legal constraints on specific technologies. While these technologies are still new, challenges may emerge as the U.S. determines if any of the information, hardware, or specific technologies should be subject to export controls; this may render certain types of collaboration untenable. Another challenge will be the impact of national data protection laws: as countries define their approach to Information Security, international partners may have data security requirements that may hamper or raise the cost of meaningful collaboration.

Budget

Like any organization allocating finite resources, AFRL must prioritize investment decisions. Developing technologies of strategic importance is not only resource intensive, but effectiveness of investment is difficult to quantify. Identifying metrics to measure effectiveness and return on investment will be a challenge and will require testing and adjustment and may vary depending on the maturity of the partnership.

Human Capital

In order to realize meaningful outcomes from international engagements, AFRL will need to ensure they have enough human capital capacity to balance staffing both national projects and emerging international projects. While the AFRL has established mechanisms to attract and retain high-quality science and engineering talent, the AFRL is still subject to the macro-trend of the national shortage of STEM personnel which may make hiring additional suitable personnel a challenge.

### L – Cybersecurity – Intel-Sharing

#### Plan drains time and resources

White House 11 The White House, “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” May 2011, <https://apps.dtic.mil/sti/pdfs/ADA543951.pdf> /GoGreen!

II. Cyberspace’s Future

Envision a future in which reliable access to the Internet is available from nearly any point on the globe, at a price that businesses and families can afford. Computers can communicate with one another across a seamless landscape of global networks permitting trusted, instantaneous communication with friends and colleagues down the block or around the world. Content is offered in local languages and flows freely beyond national borders, as improvements in digital translation open to millions a wealth of knowledge, new ideas, and rich debates. New technologies improving agriculture or promoting public health are shared with those in greatest need, and difficult problems benefit from global collaboration among experts and innovators. This, in part, is the future of cyberspace that the United States seeks—and the future we will work to realize.

In this future, individuals and businesses can quickly and easily obtain the tools necessary to set up their own presence online; domain names and addresses are available, secure, and properly maintained, without onerous licenses or unreasonable disclosures of personal information. The best engineers work together internationally to develop new standards for information systems that make networks faster and more reliable, catalyzing innovation and expanding accessibility. High-tech industry works with its customers to provide software, hardware, and services that are more secure, more reliable, and more responsive to their needs.

It is a future in which universities and companies are free to research and develop new concepts and products because they know their intellectual property and valuable data are safe, even on shared networks. Individuals know the threats to their personal computers, and can take easy-to-use measures to protect their systems. Private-sector companies also take a responsibility for their network hygiene, knowing that in so doing, they protect their investments. When cybersecurity incidents demand government action, officials can detect those threats early and share data in real-time to mitigate the spread of malware or minimize the impact of a major disruption—all while preserving the broader free flow of information. When a crime is committed internationally, law enforcement agencies are able to collaborate to safeguard and share evidence and bring individuals to justice.

This future promises not just greater prosperity and more reliable networks, but enhanced international security and a more sustainable peace. In it, states act as responsible parties in cyberspace—whether configuring networks in ways that will spare others disruption, or inhibiting criminals from using the Internet to operate from safe havens. States know that networked infrastructure must be protected, and they take measures to secure it from disruption and sabotage. They continue to collaborate bilaterally, multilaterally, and internationally to bring more of the world into the information age and into the consensus of states that seek to preserve the Internet and its core characteristics.

The United States and a growing number of partners have laid the foundation for this future already. But it is not a foregone conclusion, and we cannot build it alone. Though progress may be slow and resource-intensive, the international community must join together in support of this long-term investment. We must do so with the clear understanding that this vision of cyberspace serves national interests as much as shared international aims. The measure of our success will be another half-century of information technology as transformational as the last, as we begin to realize fully the benefits—and minimize the risks—of global interconnection.

The Future We Seek

The cyberspace environment that we seek rewards innovation and empowers individuals; it connects individuals and strengthens communities; it builds better governments and expands accountability; it safeguards fundamental freedoms and enhances personal privacy; it builds understanding, clarifies norms of behavior, and enhances national and international security. To sustain this environment, international collaboration is more than a best practice; it is a first principle.

Our Goal

The United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states’ actions, sustain partnerships, and support the rule of law in cyberspace.

Open and Interoperable: A Cyberspace That Empowers

At the core of digital innovation is the ability to add new functionality to networked machines. The openness of digital systems explains their explosive growth, rapid development, and enduring importance. Networked technology’s basic tools are steadily increasing in availability and decreasing in price, as computer and Internet access have spread to every nation. To continue to serve the needs of an ever-growing wired population, manufacturers of hardware and operating systems must continue to empower the widest possible range of developers across the globe. As companies continue to drive innovation in the development of proprietary software, we also applaud the vibrancy of the open-source software movement, giving developers and consumers the choice of community-driven solutions to meet their needs.

The United States supports an Internet with end-to-end interoperability, which allows people worldwide to connect to knowledge, ideas, and one another through technology that meets their needs. The free flow of information depends on interoperability—a principle affirmed by 174 nations in the Tunis Commitment of the World Summit on the Information Society. The alternative to global openness and interoperability is a fragmented Internet, where large swaths of the world’s population would be denied access to sophisticated applications and rich content because of a few nations’ political interests. The collaborative development of consensus-based international standards for information and communication technology is a key part of preserving openness and interoperability, growing our digital economies, and moving our societies forward.

Secure and Reliable: A Cyberspace That Endures

For cyberspace as we know it to endure, our networked systems must retain our trust. Users need to have confidence that their data will be secure in transit and storage, as well as reliable in delivery. An effective strategy will require action on many fronts, with shared responsibility at every level of society, from the end-user up through collaboration among nation-states.

Vulnerability reduction will require robust technical standards and solutions, effective incident management, trustworthy hardware and software, and secure supply chains. Risk reduction on a global scale will require effective law enforcement; internationally agreed norms of state behavior; measures that build confidence and enhance transparency; active, informed diplomacy; and appropriate deterrence. Finally, incident response will require increased collaboration and technical information sharing with the private sector and international community. This work cannot be fully addressed by any single nation or sector alone; it is a responsibility and duty that every nation, and its people, all share.

Network stability is a cornerstone of our global prosperity, and securing those networks is more than strictly a technical matter. Economically, we must advance sustainable growth and invest in infrastructure at home and abroad, while incentivizing network reliability and clarifying the obligations of firms and states. Politically, we must help to maintain an environment of respect for technical infrastructure, so disputes do not become excuses to disrupt and degrade networks. Socially, we must make end-users aware of their responsibilities to maintain and operate their devices in a safe and secure manner.

Stability Through Norms

The United States will work with like-minded states to establish an environment of expectations, or norms of behavior, that ground foreign and defense policies and guide international partnerships. The last two decades have seen the swift and unprecedented growth of the Internet as a social medium; the growing reliance of societies on networked information systems to control critical infrastructures and communications systems essential to modern life; and increasing evidence that governments are seeking to exercise traditional national power through cyberspace. These events have not been matched by clearly agreed-upon norms for acceptable state behavior in cyberspace. To bridge that gap, we will work to build a consensus on what constitutes acceptable behavior, and a partnership among those who view the functioning of these systems as essential to the national and collective interest.

The Role of Norms. In other spheres of international relations, shared understandings about acceptable behavior have enhanced stability and provided a basis for international action when corrective measures are required. Adherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict.

The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them. We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace.

The Basis for Norms. Rules that promote order and peace, advance basic human dignity, and promote freedom in economic competition are essential to any international environment. These principles provide a basic roadmap for how states can meet their traditional international obligations in cyberspace and, in many cases, reflect duties of states that apply regardless of context. The existing principles that should support cyberspace norms include:

• Upholding Fundamental Freedoms: States must respect fundamental freedoms of expression and association, online as well as off.

• Respect for Property: States should in their undertakings and through domestic laws respect intellectual property rights, including patents, trade secrets, trademarks, and copyrights.

• Valuing Privacy: Individuals should be protected from arbitrary or unlawful state interference with their privacy when they use the Internet.

• Protection from Crime: States must identify and prosecute cybercriminals, to ensure laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner.

• Right of Self-Defense: Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace.

Deriving from these traditional principles of interstate conduct are responsibilities more specific to cyberspace, focused in particular on preserving global network functionality and improving cybersecurity. Many of these responsibilities are rooted in the technical realities of the Internet. Because the Internet’s core functionality relies on systems of trust (such as the Border Gateway Protocol), states need to recognize the international implications of their technical decisions, and act with respect for one another’s networks and the broader Internet. Likewise, in designing the next generation of these systems, we must advance the common interest by supporting the soundest technical standards and governance structures, rather than those that will simply enhance national prestige or political control.

Emerging norms, also essential to this space, include:

• Global Interoperability: States should act within their authorities to help ensure the end-toend interoperability of an Internet accessible to all.

• Network Stability: States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure.

• Reliable Access: States should not arbitrarily deprive or disrupt individuals’ access to the Internet or other networked technologies.

• Multi-stakeholder Governance: Internet governance efforts must not be limited to governments, but should include all appropriate stakeholders.

• Cybersecurity Due Diligence: States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse.

While cyberspace is a dynamic environment, international behavior in it must be grounded in the principles of responsible domestic governance, peaceful interstate conduct, and reliable network management. As these ideas develop, the United States will foster and participate fully in discussions, advancing a principled approach to Internet policy-making and developing shared understandings in fora appropriate to each issue.

Our Role in Cyberspace’s Future

To realize this future and help promulgate positive norms, the United States will combine diplomacy, defense, and development to enhance prosperity, security, and openness so all can benefit from networked technology. These three approaches are central to our efforts internationally. In the latter half of the 20th century, the United States helped forge a new post-war architecture of international economic and security cooperation. In the 21st century, we will work to realize this vision of a peaceful and reliable cyberspace in that same spirit of cooperation and collective responsibility.

Diplomacy: Strengthening Partnerships

Extending the principles of peace and security to cyberspace—while preserving its benefits and character—will require strengthened partnerships and expanded initiatives. We will engage the international community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace and the actions necessary, both domestically and as an international community, to build a system of cyberspace stability.

Diplomatic Objective

The United States will work to create incentives for, and build consensus around, an international environment in which states—recognizing the intrinsic value of an open, interoperable, secure, and reliable cyberspace—work together and act as responsible stakeholders.

Strengthening Partnerships

Through our international relationships and affiliations, we will seek to ensure that as many stakeholders as possible are included in this vision of cyberspace precisely because of its economic, social, political, and security benefits. These efforts will be supported by meaningful collaboration with the private sector at home and abroad.

Distributed systems require distributed action, and no single institution, document, arrangement, or instrument could suffice in addressing the needs of our networked world. From end-users, private-sector hardware and software vendors, and Internet service providers, to regional, multilateral, and multistakeholder organizations—all are important in helping cyberspace meet its full potential.

In the international arena in particular, states have an enduring role to play in preserving peace and stability, empowering innovation, safeguarding economic and national security interests, and protecting and promoting the individual rights of citizens. In our international relations, the United States will work to establish an environment of international expectations that anchor foreign and defense policies and strengthen our international relationships.

Bilateral and Multilateral Partnerships. We will work bilaterally with nations to build collaboration on cyberspace issues important to our governments and our peoples. Building broad international understanding about cyberspace norms of behavior must begin with clear agreement among like-minded countries. We will seek a broad community of partners in these efforts, and will include cyberspace issues in a wide range of bilateral dialogues, at all levels of government and across a wide range of our activities. We will advance common action on cyberspace’s emerging challenges, while building on those enforcement tools and approaches already enjoying success. Furthermore, we will actively engage the developing world, and ensure that emerging voices on these issues are heard.

International and Multi-stakeholder Organizations. Regional organizations have been particularly effective at tackling cybersecurity problems specific to their members. They will play an increasingly important role in developing and applying norms of behavior. We will continue to use our membership in these organizations, as well as in broader international organizations, to develop productive agendas that are appropriate to each organization’s expertise and that realize concrete benefits for members. In Internet governance policy, important steps have been made to ensure responsiveness and international representation in key organizations. The United States salutes those efforts, and will continue to recognize the unique contribution of such fora that represent the entire Internet community by integrating the private sector, civil society, academia, as well as governments in a multi-stakeholder environment.

Private Sector Collaboration. Although the private sector already plays an important role in international and multi-stakeholder organizations, we will continue to leverage existing partnership mechanisms to engage with industry partners. In particular, we will work closely with infrastructure owners and operators—who are responsible for the majority of network functionality—to expand initiatives to secure the network ecosystem, preserve the benefits and character of cyberspace, avoid unnecessary impediments to technological evolution, and extend principles of peace and security. We also seek the private sector’s participation in Internet governance as essential to upholding its multi-stakeholder character, and will continue to advocate for inclusiveness in fora that take up such issues.

Defense: Dissuading and Deterring

The United States will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies. Just as importantly, we will seek to encourage good actors and dissuade and deter those who threaten peace and stability through actions in cyberspace. We will do so with overlapping policies that combine national and international network resilience with vigilance and a range of credible response options. In all our defense endeavors, we will protect civil liberties and privacy in accordance with our laws and principles.

Defense Objective

The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate.

Dissuasion

Protecting networks of such great value requires robust defensive capabilities. The United States will continue to strengthen our network defenses and our ability to withstand and recover from disruptions and other attacks. For those more sophisticated attacks that do create damage, we will act on well-developed response plans to isolate and mitigate disruption to our machines, limiting effects on our networks, and potential cascade effects beyond them.

Strength at Home. Ensuring the resilience of our networks and information systems requires collective and concerted national action that spans the whole of government, in collaboration with the private sector and individual citizens. For a decade, the United States has been fostering a culture of cybersecurity and an effective apparatus for risk mitigation and incident response. We continue to emphasize that systematically adopting sound information technology practices—across the public and private sectors—will reduce our Nation’s vulnerabilities and strengthen networks and systems. We are also making steady progress towards shared situational awareness of network vulnerabilities and risks among public and private sector networks. We have built new initiatives through our national computer security incident response team to share information among government, key industries, our critical infrastructure sectors, and other stakeholders. And we continually seek new ways to strengthen our partnership with the private sector to enhance the security of the systems on which we both rely.

Strength Abroad. This model of defense has been successfully shared internationally through education, training and ongoing operational and policy relationships. Today, through existing and developing collaborations in the technical and military defense arenas, nations share an unprecedented ability to recognize and respond to incidents—a crucial step in denying would-be attackers the ability to do lasting damage to our national and international networks. However, a globally distributed network requires globally distributed early warning capabilities. We must continue to produce new computer security incident response capabilities globally, and to facilitate their interconnection and enhanced computer network defense. The United States has a shared interest in assisting less developed nations to build capacity for defense, and in collaboration with our partners, will intensify our focus on this area. Building relationships with friends and allies will increase collective security across the international community.

Deterrence

The United States will ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits. We fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense. Likewise, interconnected networks link nations more closely, so an attack on one nation’s networks may have impact far beyond its borders.

In the case of criminals and other non-state actors who would threaten our national and economic security, domestic deterrence requires all states have processes that permit them to investigate, apprehend, and prosecute those who intrude or disrupt networks at home or abroad. Internationally, law enforcement organizations must work in concert with one another whenever possible to freeze perishable data vital to ongoing investigations, to work with legislatures and justice ministries to harmonize their approaches, and to promote due process and the rule of law—all key tenets of the Budapest Convention on Cybercrime.

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.

Development: Building Prosperity and Security

The United States will continue to demonstrate our conviction that the benefits of a connected world are universal. The virtues of an open, interoperable, secure, and reliable cyberspace should be more available than they are today, and as the world’s leading information economy, the United States is committed to ensuring others benefit from our technical resources and expertise.

Our Nation can and will play an active role in providing the knowledge and capacity to build and secure new and existing digital systems, and in so doing, build consensus among states to behave as responsible stakeholders. Building capacity to realize these goals is not a short-term expenditure, but a wise long-term investment and a commitment on the part of our government for continued engagement.

Development Objective

The United States will facilitate cybersecurity capacity-building abroad, bilaterally and through multilateral organizations, so that each country has the means to protect its digital infrastructure, strengthen global networks, and build closer partnerships in the consensus for open, interoperable, secure, and reliable networks.

Building Technical Capacity

Access to networked technology is increasingly a basic need for development. Governments and industry have made a number of meaningful steps to enhance connectivity to end-users across un-served or underserved regions. International information infrastructures continue to mature and expand, providing more nations with the opportunity to access the global flow of information. The growth of the networks worldwide, and expansion of access to them, enriches the world community, yet also presents new challenges and opportunities for collaboration on issues of traditional and cybersecurity. Much of this capacity will result from private-sector investment, and the United States will work with governments and industry to build a climate friendly to those efforts, and in which they can be leveraged to address countries’ core development needs.

Governments are a major determinant of whether this new connectivity produces positive outcomes or wastes its potential. Those states that have benefitted most from our capacity-building efforts are those that embrace technology to build prosperity and enhance social cohesion, rather than restrict access for the purposes of political control. For that reason, technical projects that the United States supports will by design enhance security and commerce, safeguard the free flow of information, and promote the global interoperability of networks.

Building Cybersecurity Capacity

Prosperity cannot be built on a foundation of fear and unreliability, and the United States is committed to helping build cybersecurity capacity alongside states’ own technological development. Enhancing national-level cybersecurity among developing nations is of immediate and long-term benefit, as more states are equipped to confront threats emanating from within their borders and in turn, build confidence in globally interconnected networks and cooperate across borders to combat criminal misuse of information technologies. It is also essential to cultivating dynamic, international research communities able to take on next-generation challenges to cybersecurity.

Acknowledging that cybersecurity is a global issue that must be addressed with national efforts on the part of all countries, we will expand and regularize initiatives focused on cybersecurity capacity building—with enhanced focus on awareness-raising, legal and technical training, and support for policy development. Such programs must address more than purely technology issues; we will work with states to recognize the breadth of the cybersecurity challenge, assist them in developing their own strategies, and build capacity across the whole range of sectors—from network security and the establishment of Computer Emergency Readiness Teams (CERTs), to international law enforcement and defense collaboration, to productive relationships with the domestic and international private sector and civil society.

Building Policy Relationships

The United States’ capacity-building assistance is envisioned as an investment, a commitment, and an important opportunity for dialogue and partnership. As countries develop a stake in cyberspace issues, we intend our dialogues to mature from capacity-building to active economic, technical, law enforcement, defense and diplomatic collaboration on issues of mutual concern. We will also facilitate relationships among countries developing cybersecurity capacity—using both regional fora and technical bodies possessing specialized expertise—and will continue to promote the sharing of best practices, lessons learned, and international technical exchanges.

III. Policy Priorities

The United States will continue to take action to help build and sustain open, interoperable, secure, and reliable networks at home and abroad, both for our citizens and others in the global community. Our approach is guided by the fundamental principles, driven by the overarching goal, and sustained by the policies outlined in this document—together they form the basis of the United States’ international cyberspace strategy.

To fully realize this future in which cyberspace lives up to its potential for all, the United States Government organizes its activities across seven interdependent areas of activity, each demanding collaboration within our government, with international partners, and with the private sector. Taken as a whole, they form the action lines of our strategic framework.

For the many departments and agencies of the United States Government already engaged in these activities, they provide reinforcement to the important work already underway. For those developing implementation plans to carry out their specific responsibilities in cyberspace, they provide context and ensure unity of effort. The policy priorities outlined here call for and guide those specific actions, highlighting areas of past, present and future emphasis that demand concerted attention and resources at the national level.

Economy: Promoting International Standards and Innovative, Open Markets

To ensure that cyberspace continues to serve the needs of our economies and innovators, we will:

• Sustain a free-trade environmentthat encourages technological innovation on accessible, globally linked networks. Just as the free flow of information is critical to the functioning of our networks, free trade helps support innovation and market growth in the information age. The global embrace of the Internet can largely be traced to the spread of lower-cost and globally available computers and network technology. Competition in these markets drives innovation, while a free-trade environment enables manufacturers to keep prices competitive and standards high. Respecting the international standards of technology development and trade is an essential part of sustaining open markets, and enables leading-edge technology companies to rapidly deliver the benefits of their innovative products and services. Over the next few decades, the globalization of technology manufacturing will only increase, with substantial benefits for our networks and consumers. The United States will work to sustain that free-trade environment, particularly in support of the high-tech sector, to ensure future innovation.

• Protect intellectual property, including commercial trade secrets, from theft. The same global networks that power innovation also open up new avenues for industrial espionage and the theft of intellectual property and commercial information. Cyberspace can be used to steal an unprecedented volume of information from businesses, universities, and government agencies; such stolen information and technology can equal billions of dollars of lost value. Individual incidents often go unreported or undetected. Results can range from unfair competition to the bankrupting of entire firms, and the national impact may be orders of magnitude larger. The persistent theft of intellectual property, whether by criminals, foreign firms, or state actors working on their behalf, can erode competitiveness in the global economy, and businesses’ opportunities to innovate. The United States will take measures to identify and respond to such actions to help build an international environment that recognizes such acts as unlawful and impermissible, and hold such actors accountable.

• Ensure the primacy of interoperable and secure technical standards, determined by technical experts. Developing international, voluntary, consensus-based cybersecurity standards and deploying products, processes, and services based upon such standards are the basis of an interoperable, secure and resilient global infrastructure. The public and private sectors must work together to develop, maintain, and implement these standards and support the development of international standards and conformity assessment schemes that prevent barriers to international trade and commerce. International cybersecurity standardization, and its voluntary and consensus-based processes, serves collective interests. They foster innovation; facilitate interoperability, security, and resiliency; improve trust in online transactions; and spur competition in global markets. The United States will foster collaboration between the public and private sector to ensure the promulgation of international standards-based requirements for products and services.

Protecting Our Networks: Enhancing Security, Reliability, and Resiliency

Because strong cybersecurity is critical to national and economic security in the broadest sense, we will:

• Promote cyberspace cooperation, particularly on norms of behavior for states and cybersecurity, bilaterally and in a range of multilateral organizations and multinational partnerships. An increasing number of international organizations are taking up cybersecurity and other cyberspace issues, and the United States continues to promote this important work, building cyberspace into their range of work to meet the needs of their varied memberships. We have worked to include relevant cyberspace issues on the agenda at the Organization of American States (OAS), the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), the Asia-Pacific Economic Cooperation Organization (APEC), the Organization for Cooperation and Security in Europe (OSCE), the African Union (AU), the Organization for Economic Cooperation and Development (OECD), the Group of Eight (G-8), the European Union (EU), the United Nations (U.N.), and the Council of Europe, and to ensure that work is supported by an effective institutional framework. The United States will continue, in these and other fora, to consolidate regional and international consensus on key cyberspace activities, including norms. We will also look to fora that enable multi-stakeholder collaboration and consensus building, to further elaborate the Internet policy principles outlined in this document. We welcome the expansion of this work to geographic regions currently underrepresented in the dialogue—most notably Africa and the Middle East—to further our interest in building worldwide capacity

• Reduce intrusions into and disruptions of U.S. networks. Unauthorized network intrusions threaten the integrity of economies and undermine national security. Agencies across the United States Government are collaborating, together with the private sector, to protect innovation from industrial espionage, to protect Federal, state, and local government networks, to protect military operations from degraded operating environments, and to secure critical infrastructure against intrusions and attacks—particularly those on energy, transportation, or financial systems, and the defense industrial base. The United States will pursue a broad international consensus of states that recognize the importance of respect for property and network stability, and will back up that conviction with our own and our partners’ willingness to defend our networks from acts that would compromise them.

• Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure. In an interconnected global environment, weak security in one nation’s systems compounds the risk to others. No one nation can have full insight into the world’s networks; we have an obligation to share our insights about our own networks and collaborate with others when events might threaten us all. As we continue to build and enhance our own response capabilities, we will work with other countries to expand the international networks that support greater global situational awareness and incident response—including between government and industry. The United States Government actively participates in watch, warning, and incident response through exchanging information with trusted networks of international partners. We will expand these capabilities through international collaboration to enhance overall resilience. The United States will also work to engage international participation in cybersecurity exercises, to elevate and strengthen established operating procedures with our partners.

• Improve the security of the high-tech supply chain, in consultation with industry. The operation of critical networks and information infrastructures depends on the assured availability of trustworthy hardware and software. Vulnerabilities in the supply chain can enable attacks on the integrity, availability, or confidentiality of networks and the data they contain. Exploitation of these vulnerabilities impairs economic performance and national security. The United States will work with industry and international partners to develop best practices for protecting the integrity of information systems and critical infrastructure. In this way, we will greatly enhance the security of the globalized supply chains on which free and open trade depend.

Law Enforcement: Extending Collaboration and the Rule of Law

To enhance confidence in cyberspace and pursue those who would exploit online systems, we will:

• Participate fully in international cybercrime policy development. The United States is committed to participating actively in discussions about how international norms and measures on cybercrime are developed bilaterally and multilaterally, in fora with proven expertise and a history of promoting effective cybercrime policies. These conversations will incorporate existing efforts, like how to extend the reach of institutions like the Budapest Convention. The United States will build these efforts upon the successful partnerships between national law enforcement agencies and the productive policy dialogues that we currently enjoy, cultivating a sense of responsibility among states joining this effort.

• Harmonize cybercrime laws internationally by expanding accession to the Budapest Convention. The United States and our allies regularly depend upon cooperation and assistance from other countries when investigating and prosecuting cybercrime cases. This cooperation is most effective and meaningful when the countries have common cybercrime laws, which facilitates evidence-sharing, extradition, and other types of coordination. The Budapest Convention on Cybercrime provides countries with a model for drafting and updating their current laws, and it has proven to be an effective mechanism for enhancing international cooperation in cybercrime cases. The United States will continue to encourage other countries to become parties to the Convention and will help current non-parties use the Convention as a basis for their own laws, easing bilateral cooperation in the short term, and preparing them for the possibility of accession to the Convention in the long term.

• Focus cybercrime laws on combating illegal activities, not restricting access to the Internet. Criminal behavior in cyberspace should be met with effective law enforcement, not policies that restrict legitimate access to or content on the Internet. To advance this goal, the United States Government works on a bilateral and multilateral basis to ensure that countries recognize that online crimes should be approached by focusing on preventing crime and catching and punishing offenders, rather than by broadly limiting access to the Internet, as a broad limitation of access would affect innocent Internet users as well. As the United States and our partners engage in dialogue and help build capacity among law enforcement organizations worldwide, we will integrate this approach, uniting protection of privacy, fundamental freedoms, and innovation with collaboration to combat crimes in cyberspace.

• Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks. The United States has a variety of international capacity-building and training programs on cybercrime, helping law enforcement and legislators develop effective legal frameworks and expertise to investigate and prosecute terrorist and other criminal misuse of the Internet. Preventing terrorists from enhancing capabilities through “hackers for hire” and organized crime tools is an important priority for the international community, and demands effective cybercrime laws. The United States is committed to tracking and disrupting terrorist and cybercrime finance networks through technical tools and international cooperation frameworks such as the Financial Action Task Force.

Military: Preparing for 21st Century Security Challenges

Since our commitment to defend our citizens, allies, and interests extends to wherever they might be threatened, we will:

• Recognize and adapt to the military’s increasing need for reliable and secure networks. We recognize that our armed forces increasingly depend on the networks that support them, and we will work to ensure that our military remains fully equipped to operate even in an environment where others might seek to disrupt its systems, or other infrastructure vital to national defense. Like all nations, the United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so.

• Build and enhance existing military alliances to confront potential threats in cyberspace. Cybersecurity cannot be achieved by any one nation alone, and greater levels of international cooperation are needed to confront those actors who would seek to disrupt or exploit our networks. This effort begins by acknowledging that the interconnected nature of networked systems of our closest allies, such as those of NATO and its member states, creates opportunities and new risks. Moving forward, the United States will continue to work with the militaries and civilian counterparts of our allies and partners to expand situational awareness and shared warning systems, enhance our ability to work together in times of peace and crisis, and develop the means and method of collective self-defense in cyberspace. Such military alliances and partnerships will bolster our collective deterrence capabilities and strengthen our ability to defend the United States against state and non-state actors.

• Expand cyberspace cooperation with allies and partners to increase collective security. The challenges of cyberspace also create opportunities to work in new ways with allied and partner militaries. By developing a shared understanding of standard operating procedures, our armed forces can enhance security through coordination and greater information exchange; these engagements will diminish misperceptions about military activities and the potential for escalatory behavior. Dialogues and best practice exchanges to enhance partner capabilities, such as digital forensics, work force development, and network penetration and resiliency testing will be important to this effort. The United States will work in close partnership with like-minded states to leverage capabilities, reduce collective risk, and foster multi-stakeholder initiatives to deter malicious activities in cyberspace.

### L – Cybersecurity – Hybrid War

#### Plan’s an enormous drain on resources

Sanger 16 David E. Sanger, White House and national security correspondent and senior writer at The New York Times, senior fellow in The Press and National Security at the Belfer Center for Science and International Affairs at Harvard, graduate of Harvard College, “As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy,” New York Times, 6-16-2016, <https://www.nytimes.com/2016/06/17/world/europe/nato-russia-cyberwarfare.html> /GoGreen!

Two years ago, NATO declared that it could rule a cyberattack on one of its member states to be the equivalent of an armed attack, which would lead to a commitment by all NATO members to respond.

But when it comes to deterring the kinds of low-level probes, espionage and attacks that flow through European computer networks every week, NATO commanders do not seem prepared to take aggressive countermeasures.

Jens Stoltenberg, the NATO secretary general, has taken a low-key, purely defensive view of what the alliance should do in cyberspace. In an interview with the German newsmagazine Der Spiegel last week, he talked of sharing information and expertise, but nothing of the kind of sophisticated probing and early-warning deterrence strategies that large and small powers have begun to develop.

In short, it sounded like a strategy from a previous age, before cyberattacks were regularly used as a weapon and as a tool of espionage.

James Lewis of the Center for Strategic and International Studies in Washington, who has written about how NATO could use offensive cyberweapons, said there was “a huge reluctance to share capabilities.” The United States and Britain say little about their offensive cyberweapon abilities, even to their NATO allies.

“The Russians get that,” Mr. Lewis said. “And they know that there is lots they can do without triggering any response.”

In part, that is because the Russians are experts at hiding their tracks. Almost all of the studies of the Ukraine power grid attack in late 2015 — both unclassified and classified — have pointed to hackers in Russia. But American intelligence officials say they have never been able to track the blackout, which affected 225,000 Ukrainians, directly to Mr. Putin’s government, and probably never will.

Instead, American officials are giving cyberutility firms and cybersecurity groups around the United States confidential presentations of an analysis of what happened to the Ukrainian utilities, as a warning of what could occur on home soil.

At United States Cyber Command, which has expanded rapidly since the United States carried out cyberattacks against Iran in 2010, Russia’s networks are a regular target of surveillance. By next year, Cyber Command will have more than 130 teams fully in operation around the world, integrated into Army, Navy, Marine and Air Force units, in addition to teams that work alongside the National Security Agency at Fort Meade, Md.

It has built up a vast early warning network, placing tens of thousands of “implants” — sensors that can also be used to insert malware — into networks around the world. But NATO is only beginning to explore what it delicately calls “active defense,” and says it is not focused on offensive cyberweapons.

The Russians have no such compunctions. But it is unclear what Russian hackers hope to achieve here in the Baltics, other than to make the point, as they did in 2007 when they brought Estonia to an electronic halt, that they can get into any system, anytime.

“Whatever the Russians have in mind — mostly intimidation — it usually fails,” said Estonia’s president, Toomas Hendrik Ilves, who grew up in New Jersey before coming here to turn this small NATO country into a pioneer in introducing new web-based technology for governing a nation. The 2007 attacks backfired, he noted, because they drove Estonians far more solidly into the European and NATO camps.

In Sweden and Finland, neutral nations in the Cold War, the politics are more complex. As the NATO exercise began in Finland last week, the Finnish foreign minister was in Moscow, meeting his Russian counterpart, Sergey V. Lavrov.

The more Sweden and Finland turn to NATO, the more their networks, their news sites and their government ministries come under cyberattack. As Adm. John Richardson, the chief of United States naval operations, said at an event at the Council on Foreign Relations in May, “The fact is it’s a pretty hot war in the cyber domain going on right now.”

A hot war, but a kind that suits Russia well: It is part of what military strategists call “gray zone” combat. For Mr. Putin, cyberespionage and cyberattacks keep NATO and its partners off balance. They are enormously difficult and expensive to defend against, and, at least for now, they have operated below the line that is likely to prompt a military or economic response.

“It stays below the radar,” Martin Libicki of the RAND Corporation told a conference sponsored this month by the NATO cyber center here, officially known as the NATO Cooperative Cyber Defense Center of Excellence.

For the Russians, Mr. Libicki said, cyberespionage and weaponry are part of a larger strategy of information warfare and a blitz of propaganda that makes sorting out fact from fiction — say, the causes of the Malaysia Airlines crash in Ukraine — all the more difficult. But the attacks also remind the smaller nations here of their vulnerability, even if Russia’s troops stay on their side of the border.

So far, NATO has found few effective means of deterring attacks.

“The biggest problem in cyber remains deterrence,” said Mr. Ilves, the Estonian president, who has made the issue of avoiding cyber conflict one of the main themes of his time in office. “We have been talking about the need to deal with it within NATO for years now.”

His fear, he said, is that Russia or other cyberattackers will soon move to the next frontier: subtle manipulation of data like medical records, the operations of weapons systems and navigation data.

But for now, Europe’s focus is on keeping its secrets safe and its weapons working. Germany issued a warning last month about Russian attacks; its Parliament was targeted last year in an operation that sought to install software that would have given Russia continuous access to the Parliament’s computer networks. Hans-Georg Maassen, the head of the German domestic intelligence agency, told The Financial Times that the Russians were “showing a readiness for sabotage.”

Now, Germany’s defense agency has done what NATO has not: It has started its own cyberwarfare unit.

### L – AI

#### Plan drains significant resources

Christie 22 Edward Hunter Christie, senior research fellow at the Finnish Institute of International Affairs, owner of AI Policy Consulting, former NATO deputy head of the Innovation Unit, “Defence cooperation in artificial intelligence: Bridging the transatlantic gap for a stronger Europe,” European View, 21(1), 3-31-2022, pp.13-21, [DOI](https://journals.sagepub.com/doi/full/10.1177/17816858221089372) [10.1177/17816858221089372](https://doi.org/10.1177/17816858221089372) /GoGreen!

Much has already been achieved in terms of new structures, new initiatives and new policy developments to support the collaborative adoption of AI among NATO Allies and EU member states. In addition to pre-existing structures and mechanisms at both the NATO and EU levels, which have ensured that nations are not starting from scratch, national defence institutions are already able to refer to common policy commitments and to options, whether through NATO or the EDA, for research or capability-development activities. At the same time, ensuring a competitive edge in AI is a truly whole-of-government effort which requires considerable cross-over between the military and civilian realms.

Large gaps remain between the US and the EU on certain key indicators. At the same time, the gaps pertaining to research are far smaller. To ensure greater European performance and relevance in AI in general, and its defence applications in particular, it seems desirable to focus on two strategic priorities: investment volumes, both public and private, which need to be significantly increased; and the full use of collaborative mechanisms involving the US.

To that end, it would be beneficial for nations on both sides of the Atlantic to ensure that a clear and common vision is set out in forthcoming strategic documents, most notably the EU’s Strategic Compass and NATO’s new Strategic Concept. This should include clear political commitments to increasing investment, both in general and in instruments for promoting collaborative innovation. There are opportunities for ‘more Europe’ through the EDA and the European Defence Fund. But while pursuing those avenues, European capitals should prioritise efforts that complement and enhance transatlantic approaches, in recognition of the reality that the US remains the indispensable ally for Europe’s security.

### L – Biotech

#### Plan drains significant resources

Goodman 21 Matthew P. Goodman, senior vice president for economics and Simon Chair in Political Economy at the Center for Strategic and International Studies; and Brooke Roberts, research associate with the Economics Program at CSIS; “Toward a T12: Putting Allied Technology Cooperation into Practice,” CSIS Brief, 10-13-2021, <https://www.csis.org/analysis/toward-t12-putting-allied-technology-cooperation-practice> /GoGreen!

The effectiveness of any technology alliance will depend on prioritization. Allies cannot work together on every new technology or address every issue that either enables or impedes cooperation. They will have to make choices, particularly on two questions: Which technologies are most critical for—and amenable to—allied cooperation? And where along the chain of technology development are the greatest opportunities for—and obstacles to—allied cooperation?

WHICH TECHNOLOGIES?

In his first major speech as President Biden’s national security adviser, Jake Sullivan highlighted four sectors that will define what he called “the third wave of the digital revolution”: AI, biotechnology, semiconductors, and telecommunications. This is a reasonable list around which to explore the possibility for allied cooperation. These sectors increasingly shape how we make decisions, how we physically live and breathe, how we power technology, and how we communicate. The potential for growth and innovation in these four areas over the next decade or two is enormous. They are also technologies on which international competition is likely to be most intense—and on which the benefits of cooperation are potentially greatest. China, in particular, has set its sights on global preeminence in all four of these areas.

Each of these areas has great potential for expanded cooperation among allies:

AI refers to the creation of smart machines that can mimic human learning and thought-process capabilities. This technology allows machines to operate human-run tasks, potentially improving the cost, accuracy, and efficiency of these activities. China is dedicating significant state resources toward AI tech development, with potentially troubling commercial and military implications for the United States and its allies. There is a solid foundation for allied cooperation on AI. Research collaboration in this area is already well established, including a formal partnership between the U.S. National Science Foundation and the Natural Sciences and Engineering Research Council of Canada on technology research, of which AI is an important component, and the 2020 U.S.-UK declaration to further cooperation in AI R&D. Expanding this kind of research collaboration, particularly on scaling and commercializing AI technologies, could help get allied AI products to market and ensure they are competitive with Chinese alternatives. Moreover, there are several useful international policy frameworks on which to build out allied cooperation. These include the G7-led Global Partnership on Artificial Intelligence (GPAI), the Organization of Economic Cooperation and Development’s (OECD) Principles on AI, and AI provisions in regional trade arrangements, including the Singapore-led Digital Economy Partnership Agreement (DEPA).

Biotechnology, the creation of products through biological materials or processes, has enormous potential for solving health, agriculture, and environmental challenges. Moreover, one of the most important areas of potential for biotech lies in its ability to transform the manufacturing sector. Biomanufacturing—the application of biotech in manufacturing—will allow countries to not only create different types of products but to do so in new, more sustainable ways. For example, Cambium BioMaterials, a Bay Area start-up, recently biomanufactured an enhanced flame-retardant material using plant-based ingredients that is now being used in commercial and military grade. China, the world’s leading manufacturer, already dedicates significant resources to support innovation in biotech, for potential commercial and military purposes. Allied cooperation on biotech is nascent at this point, but the United States, Germany, Singapore, and Israel are notable leaders in the field, and there is significant scope for building out collaboration.

Semiconductors are “the brains of modern electronics.” They control the flow of electrical currents in electronic devices, making them a critical component of the technologies of both today and tomorrow. And as the world’s digital transformation accelerates, so does the demand for semiconductors. The world needs more large-scale semiconductor production facilities to meet this demand, but because it is increasingly expensive and complex to produce semiconductors, no one country can solely support this expansion. The semiconductor industry is already one that benefits from specialization—and cooperation—across allies and partners, with the United States dominating front-end research and design, and East Asian countries—including Taiwan, South Korea, and Japan—leading the manufacturing segment of the supply chain. Yet China has set its sights on assuming global leadership in advanced semiconductor manufacturing, as detailed in Beijing’s 2014 Guidelines to Promote National Integrated Circuit Industry Development. In response to that and other foreign government subsidy programs for semiconductor development, the U.S. Congress enacted the Creating Helpful Incentives to Produce Semiconductors for America (CHIPS) Act in the 2021 National Defense Authorization Act. If funded, this would direct $52 billion of federal money toward domestic semiconductor manufacturing and R&D. The Biden administration has supported the CHIPS Act as critical to sustaining U.S. competitiveness in semiconductors, but it will also be important to enhance cooperation with allies and partners on this foundation technology.

Telecommunications—the transmission of data via wire, radio waves, optical fiber, and other means—are the backbone of today’s interconnected economy. The technology underlying telecom networks has advanced rapidly in the past two to three decades through several “generations.” The global market for telecom equipment is dominated by a handful of vertically integrated suppliers such as Huawei and ZTE of China, Ericsson of Sweden, and Nokia of Finland. The sector is highly susceptible to first-mover advantages; the first company to deploy the latest generation network (5G) doesn’t have to compete with other companies for subscribers and network partners, amassing large shares of both and making it easier for the company to deploy other technologies (telecom equipment, phones, radios, etc.) to their subscribers and network partners. China has moved aggressively in international forums and markets to try to harness the first-mover advantage by setting standards that favor its telecom networks and equipment. This poses a critical challenge to the United States and allied countries, particularly in their ability to secure competitive market shares for their telecom and other network-dependent technology. Allied efforts are already underway to try to diminish the impact of the first-mover advantage by promoting the use of the Open Radio Access Network (O-RAN) platform, which is not reliant on supplier-specific software or hardware. The O-RAN Alliance, a group of over 270 telecommunications operators and vendors that are dedicated to creating “fully interoperable mobile networks,” and the Open RAN Policy Coalition, a group of 60 technology companies from around the world dedicated to the advancement and adoption of open RANs, are critical groups of allied companies working to foster a collaborative environment for telecommunication technology. The United States and Japan have been particularly active in their efforts to innovate in telecoms and compete with China, notably through joint investments in 6G development under the countries’ newly launched Global Digital Connectivity Partnership. Allied efforts in telecommunications can help expand these efforts and increase O-RAN adoption.

WHERE TO FOCUS COOPERATION?

After agreeing on the technologies to prioritize, allies will need to decide how to direct their efforts along the technology development chain and what substantive issues to focus on. There are opportunities to expand cooperation across a range of activities, from research collaboration to joint financing. In roundtables and conversations with experts conducted by the CSIS Economics Program as part of this project, two cross-cutting issues repeatedly came up: data and standards. Focusing allied efforts on aligning approaches in these two areas would make a significant contribution to joint promotion of critical technologies.

After agreeing on the technologies to prioritize, allies will need to decide how to direct their efforts along the technology development chain and what substantive issues to focus on.

Data

In 2020, the world generated some 44 zettabytes of data—“40 times more bytes than there are stars in the observable universe.” Data are everywhere, fueling technology and informing our decisions and innovation choices. In biotechnology, for example, data analytics help biopharmaceutical researchers identify drug candidates for early-stage testing and drug development. Progress in AI development is largely a function of data and the computing power to process it.

These and similar innovations are dependent on data quantity, quality, and diversity—how much data one has, how accurate and usable those data are, and how many different types of data are available. As the Global Data Alliance, an industry coalition, notes, greater data quantity allows researchers and firms to “identify meaningful insights, patterns, and connections that can aid R&D teams in discovering and developing novel solutions to scientific and technical challenges.” Access to high-quality data enables faster, more reliable discoveries. Data diversity helps researchers and firms broaden these discoveries, applying them to new products, patients, and processes.

Data are essential to allied technology efforts for the seemingly simple reason that sharing data is beneficial. Sharing increases the quantity of data and therefore the potential for new discoveries. But it also improves the quality of data, by allowing entities to verify their data against data held by others and to inform, supplement, and complement their data. Sharing data can also increase the diversity of data sets, allowing researchers and producers to apply their results to a wider range of products and demographics. This is especially important in the development of AI, where access to different types of data allows machines to make better decisions.

For all the benefits of data sharing, a number of frictions impede allied cooperation in this area. These include national laws and policies to protect the privacy and security of sensitive data. Every government has a legitimate interest in ensuring that sensitive personal, business, and government information does not get into the wrong hands, and law and policy in this area nearly always restrict the use and sharing of this data in some ways. The problem is when these restrictions inhibit reasonable, responsible, and ethical data sharing with organizations in like-minded countries involved in joint research projects. There are emerging differences in national philosophies and regulatory approaches to data privacy and security that complicate, or may preclude, allied data sharing in support of joint promotion of critical technologies.

As mentioned earlier, the European Union considers personal data privacy a human right and has put into law what is arguably the global standard for data protection in its General Data Protection Regulation (GDPR). Several other countries have enacted data laws based on GDPR, including South Korea and India. For its part, the United States has a patchwork of privacy rules at the state and sectoral level but no comprehensive federal legislation in this area. By contrast, data security has taken on new salience in Washington, as highlighted by President Biden’s signing of an executive order in this area in June. How this will affect Washington’s historic position that data should generally flow freely across borders remains to be seen.

Meanwhile, several allied and partner countries have also enacted data localization policies, which require data to be stored domestically. This can silo data within states, impede data flows, and undermine innovation. According to a report by the Information Technology and Innovation Foundation (ITIF), as of 2020, 62 countries had enacted 144 data localization policies. Many governments such as the European Union and South Korea claim that data localization is necessary to protect “important” or “sensitive” data from being shared; U.S. financial regulators take a similar view with respect to financial data. However, localization policies are often broadly applied and seem to be less about legitimate protection than about protectionism.

Efforts to bridge the differences among allies on data flows, privacy, and security have so far had mixed success. Japan has usefully put forward the concept of “data free flow with trust (DFFT)” and won both G7 and G20 endorsement of the idea, but it has yet to be turned into an agreed set of rules and practices. To facilitate data flows across the Atlantic, the United States and the European Union negotiated a “privacy shield” in 2016, providing a mechanism for companies to comply with GDPR regulations when transferring data from Europe to the United States. However, in 2020, the European Court of Justice found that the framework failed to meet GDPR standards and subsequently invalidated the policy. Without a replacement framework, transatlantic technology cooperation will be constrained.

More positively, as detailed in a CSIS report in April 2021, there has been useful work on developing agreed approaches to data governance in a number of recent trade agreements, particularly among U.S. partners in the Asia-Pacific region. The U.S.-Mexico-Canada Agreement (USMCA) incorporates and builds on commitments to substantially free cross-border data flows and other rules the United States won agreement to in the Trans-Pacific Partnership (TPP) before it pulled out in early 2017. Similar provisions were included in the U.S.-Japan Digital Trade Agreement concluded in 2019. And Singapore has been a leader in aligning data governance policies through its bilateral trade agreements, in the Asia-Pacific Economic Cooperation (APEC) forum and through its innovative DEPA arrangement.

Moving forward, to capitalize on the innovation gains that come from sharing data and promote meaningful allied technology cooperation, the Biden administration should focus on several lines of effort to reconcile the divergent approaches to data governance among its key allies. First, it should work with Congress to enact comprehensive federal privacy legislation. Second, it should use the new TTC forum with the European Union to align transatlantic positions on data privacy, security, and flows. Third, it should embrace the work on data governance in the Asia-Pacific region, starting by docking onto DEPA. And fourth, it should work to identify areas where U.S. agencies can pool data with like-minded countries in the interest of conducting joint research on issues of mutual concern. (For example, NIST could combine data with UK or EU counterparts to improve the accuracy of facial recognition tests.) These efforts will help improve the quantity, quality, and diversity of allied data sets, enabling greater innovation opportunities for allied researchers and firms in critical sectors such as AI, biotech, semiconductors, and telecommunications.

Standards

The term “standards” is used to describe a broad array of rules, metrics, and norms, ranging from ubiquitous technical specifications like Bluetooth to safety requirements such as the warning labels found on lawn mowers to expected approaches that establish a certain baseline such as in accounting standards. In all these variations, standards convey a sense of expectation of performance. There are broadly two types of standards: consensus standards and technical regulations. Consensus standards are the outcomes of processes where general agreement rather than unanimity is sought and the development of such outcomes is voluntary. Technical regulations refer to the use of standards by the government to meet a specific policy objective and where conformance with the standard is mandatory.

Standards are critical to innovation for two reasons: first, they provide a foundation for technology development upon which product differentiation can be made, which makes it easier to deploy competitive products, including by leveraging first-mover advantages; and second, they boost product interoperability and consumer confidence in technologies, expanding existing technology markets and helping to create new ones. The focus here is mainly on voluntary standards because, as with data governance, there is arguably more work to be done to align allied approaches.

Global standards are typically set in a broad range of bodies that are open to participation by all interested stakeholders and where decisionmaking is done by consensus. Examples of such as bodies include the International Organization for Standardization (ISO), the Third Generation Partnership Project (3GPP), and the Institute of Electrical and Electronics Engineers (IEEE). Participants in these bodies include a mix of government and private-sector researchers and other experts from the member countries. The process for reaching agreement on standards varies by organization, with different thresholds in balloting that help establish consensus.

As is the case with data governance, the United States and its allies have different approaches to standard setting. While government agencies such as the National Institute of Standards and Technology (NIST), the Department of Defense, and the Department of Transportation participate in many standard-setting bodies, Washington does not lead in setting technical standards. It is the long-standing policy of the United States to allow the private sector to take the lead, leveraging the extensive technical expertise and experience available in industry and its knowledge of market need and demands. This private-sector–led approach—in which the U.S. government participates as a contributor, user, and enforcer—has helped establish and maintain U.S. industrial and technological leadership since World War II. By contrast, governments in Europe and Asia tend to have a top-down approach to standard setting, establishing standardization priorities and attempting to develop and protect domestic champions. In order to achieve these objectives, these governments often send a large number of officials to push for preferred national outcomes.

While there is a strong case for the U.S. government to step up its long-term game in international standard setting—for example, by investing in and adequately resourcing government experts to participate in global standards work—the likelihood that the United States and its allies will align their approaches in standard-setting bodies is low. In addition to the philosophical differences, these countries are also competitors and want their own companies and technologies to “win” in the marketplace. There are numerous examples of such competition in emerging technologies such as cloud computing, cybersecurity, and advanced manufacturing. Moreover, the industry-led U.S. approach, with its competitive dynamics among actors who have a better sense of the market potential of new technologies than governments, arguably has real advantages over the top-down approach used by Europe and other allies.

A more productive line of effort for U.S. policymakers seeking to promote greater allied alignment in the technical standards would be to encourage pre-standardization cooperation. Here it is useful to explore the concept of “technology readiness levels (TRLs).” These measure the maturity of technology along a spectrum from early-stage basic research to commercialization and deployment of technology. The lower the TRL, the less developed the technology and the greater the need is for fundamental research and development. Collaboration at low TRLs—basic research—is already well established. International standard setting happens at higher TRLs, where, as discussed above, allied cooperation faces a number of challenges. The opportunity lies in the middle of the TRL spectrum, where governments could help researchers collaborate on basic research and develop shared insights and data and, by so doing, set the stage for more productive standards cooperation and, even further along the technology-development spectrum, promote regulatory convergence among allies.

In addition to encouraging pre-standardization cooperation, Washington could do more to engender trust and cooperation with the private sector on standard setting and related policies. With its extensive firsthand experience, the private sector can help the government better understand the true dynamics of standard-setting rivalries in different standards bodies. Greater public-private exchange of perspectives on the commercial and national security dimensions of emerging technologies would also be valuable. Also, as mentioned above, small amounts of additional funding for government experts’ participation in—though not direction of—international standard-setting work could improve public-private coordination and support U.S.-preferred outcomes.

While the focus here has mainly been on technical standards, it is also important for the U.S. government to work closely with allies on aligning regulatory approaches to technology. In addition to promoting positive U.S.-preferred norms such as environmental and social sustainability of technology, these efforts would help minimize the scope for misuse or ethical breaches of new technologies. The OECD Principles on AI, for example, are designed to ensure that development of AI technologies adheres to global democratic and human rights values. The International Bioethics Committee (IBC), housed under UNESCO, is another body working to develop normative requirements to safeguard human rights in the development and use of biotechnologies.

Getting Organized

Promotion of critical technologies is a complex and challenging undertaking, even within a single country. The challenges are compounded when coordinating efforts with other countries. An effective technology alliance will require organizational structures and processes—both within the United States and across allies and partners—that maximize the benefits of cooperation and remove or overcome obstacles.

Effective organization starts at home. The Biden administration has taken some useful first steps in this regard. They have rhetorically made the case for promotion and protection of critical technologies and for coordinating these efforts with allies. The White House has created a new senior position in the National Security Council staff for technology policy coordination and has elevated the head of the Office of Science and Technology Policy (OSTP) to cabinet level to improve internal U.S. government coordination. And it has made technology cooperation a top agenda item for plurilateral forums of like-minded countries such as the Quad and G7, as well as in bilateral engagement with Europe, Japan, and other technology partners. Meanwhile, the U.S. Congress has taken steps to provide legislative and financial support for allied technology cooperation, including through measures such as the U.S Innovation and Competitiveness Act (USICA) passed by the Senate in June.

An effective technology alliance will require organizational structures and processes—both within the United States and across allies and partners—that maximize the benefits of cooperation and remove or overcome obstacles.

However, there are still gaps and inconsistencies in Washington’s efforts at home to set the groundwork for a technology alliance. Announcing a new policy direction is one thing; carrying it out in a sustained and consistent way is far more challenging. This requires a well-functioning interagency process under the direction of the White House that deploys relevant parts of the U.S. government. The Biden administration has been slow to appoint senior officials at the under- and assistant-secretary level at key economic agencies, who are critical to effective policy formulation and implementation. Even when these officials are in place, they need to be empowered to do the day-to-day work of coordinating policy with allies, with direction—but not micromanagement—from the White House.

Moreover, Washington needs to make important substantive investments at home if it wants to win support from allies for its positions on the cross-cutting issues discussed above. To promote its preferred approach to global data governance, for example, the United States needs to enact comprehensive federal privacy legislation. It needs to revitalize the U.S. approach to standard setting, doing more to support the efforts of private companies and experts in this area. And it needs to recommit to the U.S. innovation base by, among other things, increasing federal R&D spending, investing in skills, and building digital infrastructure. (Detailed recommendations in these areas were included in the CSIS Trade Commission’s October 2020 report, Sharpening America’s Innovative Edge.)

One more chore for the Biden administration is to reconcile the tension between its appeal to allies for technology cooperation, on one hand, and its stated preference to “buy American” and to onshore production of critical technologies and supplies, on the other. Allies will be reluctant to sign onto cooperation if they have doubts about what is in it for them. This is an even more pointed question for allies still subject to tariffs imposed by the Trump administration.

Progress on these domestic organizational and messaging challenges will need to be complemented by work to organize international cooperation on technology promotion. Again, the Biden administration has made a good start on agenda setting in the Quad and G7 and with bilateral partners such as Japan, South Korea, and Germany. It has wisely avoided calling for a single T12 forum with a predetermined group of countries; the kind of “variable geometry” it has been promoting is more suited to an issue area with a complex mix of critical technologies and country capabilities.

But there is still work to be done to stitch all these strands together. It is especially important for Washington to resolve its differences with Europe over the regulation of technology and data, or at least to close the gap enough to align transatlantic (essentially, G7) and transpacific (Quad) approaches to these issues. It will also be important to pull in other economies as needed that are not in the Quad or G7 but have advanced capabilities in key technologies—such as the Netherlands, South Korea, and Taiwan on semiconductors or Finland and Sweden on 5G—without making the web of allied cooperative efforts too cumbersome.

With more alignment of key players within a technology alliance, Washington will then want to reinforce and build out work in international institutions in which it retains disproportionate influence to develop U.S.-preferred rules, standards, and norms. NATO and the OECD have done useful work to promote common principles on AI, for example; the latter has also done important work on data governance. Allies will also need to align positions in standard-setting bodies with a more diverse membership such as the International Telecommunication Union.

Conclusion

There are many other important lines of effort needed to promote allied technology cooperation that strengthens U.S. and allied competitiveness and national security. In a thoughtful article in Foreign Affairs in October 2020, Jared Cohen and Richard Fontaine outlined a number of other priority technologies for cooperation—including quantum computing, drones, and financial technology—as well as potential forms of collaboration—joint assessments of risk, coordinating investments in R&D, and even aligning education and immigration policies. And as mentioned earlier, the protection side of the ledger also requires work to align allies’ export control, investment screening, and other technology control policies. But the White House needs to start somewhere, and encouraging collaboration among relevant groups of allies and partners on the four technologies, two cross-cutting issues, and various organizational steps identified in this brief would be a good place to focus initial efforts and begin building an effective T12.

### L – Exercises

#### Field exercises are particularly resource-intensive

DoD 21 Defense Security Cooperation University, Defense Security Cooperation Agency, U.S. Department of Defense, “Chapter 1 Introduction to Security Cooperation,” Security Cooperation Management (aka DSCU Green Book), Edition 41.0, May 2021, https://www.dscu.edu/documents/publications/greenbook/v41\_0/24\_Greenbook\_41\_0\_Complete.pdf /GoGreen!

Exercises

Combined exercises are exercises between the U.S. forces and those of one or more countries. It is common error to refer to these exercises as multinational, coalition, or joint operations, but this is doctrinally incorrect. It should be noted that the term “joint” refers to two or more services, e.g., Army and Air Force. Exercises can be both joint and combined, while most combined exercises are single-service combined exercises. The primary purpose of combined exercises is the training of U.S. forces, emphasizing interoperability and capability building, though the host nation also benefits from the training as well. There are three types of exercises that may fall under this title:

• Field Training Exercises (FTX): These are the most realistic of exercises, taking the form of actual forces in the field, thus allowing all the moving parts to be tested. These are also the most resource intensive in money, manpower, material, and preparation time.

• Command Post Exercises (CPX): An exercise in which the forces are simulated, involving the commander, the staff, and communications/coordination among the participating headquarters.

• Table Top Exercises (TTX): Tabletop exercises are the least resource-intensive of these three types, ranging from a formal, detailed planning process to a simple discussion. TTXs are excellent when senior leaders want to explore a number for possible scenarios or possible futures.

#### So are command post and table-top exercises

O’Mahony 18 Angela O’Mahony, associate dean for academic affairs at Pardee RAND Graduate School and a senior political scientist at RAND, former assistant professor of international political economy and economic statecraft at the University of British Columbia, PhD political science, UCSD; Ilana Blum, researcher at RAND; Gabriela Armenta, researcher at RAND; Nicholas Burger, senior economist at RAND and director of RAND’s Washington office; Joshua Mendelsohn, researcher at RAND; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Steven W. Popper, researcher at RAND; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; and Thomas S. Szayna, senior political scientist and former director of RAND's Defense and Political Sciences Department at RAND, MA international relations, Claremont Graduate School; “Assessing, Monitoring, and Evaluating Army Security Cooperation: A Framework for Implementation,” RR2165, RAND Corporation, 2018, <https://apps.dtic.mil/sti/pdfs/AD1056354.pdf> /GoGreen!

Figure S.6 presents a truncated version of this decision tree. In it, we present a notional M&E strategy for Southern Accord, a multilateral exercise held by U.S. Army Africa. We present this example in more detail in Appendixes D and E. As an initial check, the decision tree ties all M&E decisions to planners’ TOCs (boxes 1 and 2). Three decision nodes guided the notional path we outline for Southern Accord. First, is this a recurring activity (box 5)? Southern Accord is a recurring series of multilateral activities, but each one is relatively unique in its execution. As a result, we expect that most planners will view Southern Accord as a nonrecurring activity. In contrast, most training courses would be recurring activities. Second, is this a resource-intensive activity (box 6)? Historically, Southern Accord is a command post and tabletop exercise, which are generally considered medium-cost training exercises—they are much more resource intensive than subject matter exchanges, but are dwarfed by an undertaking such as Pacific Engagement. Third, is this activity a priority? Based on discussions with U.S. Army Africa planners for previous RAND research, Southern Accord was identified as a priority activity.5 Southern Accord, and its associated African Land Forces Summit, provides a valuable forum for U.S. Africa and regional leaders to engage. Based on these decision nodes, we recommend that an activity such as Southern Accord incorporate a monitoring strategy in the activity implementation.

### AT: N/L – Plan Cheap

#### Price tags are misleading – that’s the whole point – without AM&E, costs balloon through inefficiency, mismanagement, and extortion

Munson 13 Peter J. Munson, senior vice president for preventive services and global crisis management for a private sector corporation, retired U.S. Marine Corps officer, “The Limits of Security Cooperation,” War On The Rocks, 9-10-2013, <https://warontherocks.com/2013/09/the-limits-of-security-cooperation/> /GoGreen!

If SC is incapable in many cases of building meaningful partner capacity or creating real influence, then wonks will argue that SC and especially military aid payments are needed to secure much more black-and-white U.S. interests: overflight and transit agreements and peace treaty compliance. Yet, this is another instance where the bankruptcy of SC ideology is demonstrated. SC funding and services are generally not initiated as a quid pro quo for overflight and transit. Once the flow of cash has started, however, threats of closing off cooperation in the form of overflight, transit, or other agreements become tools of extortion in the hands of the foreign partner. No matter how inefficient or expensive, the U.S. cannot turn the spigot down or off. SC thus is not a tool to condition partner behaviors, but rather an entitlement—a fee for maintaining the status quo—a baseline bribe that creates a market of fees-for-service for the most mundane issues.

SC does work to build capacity in certain, relatively elite units that perceive a real need for improvement and hard training. Likewise, it works to build interoperability between already-capable partner forces and U.S. and coalition militaries. SC in the right doses can be a good way of showing solidarity with allies against other regional threats. But SC is not a panacea and must be applied with significantly more discernment than the usual some-is-good-more-is-better logic of U.S. military spending.

Planners should go to great lengths to ensure that SC is seen as a tool for a specific purpose, not a reward to condition behaviors. SC-as-a-conditioning-tool becomes bribery with diminishing returns. If policymakers want a quid pro quo, they need to admit as much and use much more precisely targeted incentives: paying a fee for access or head-of-the-line transit privileges for example. This becomes a much more predictable business transaction than trying to use SC funds, winks, and nudges to get one’s way.

Finally, in the land of perverse incentives, SC is often seen as a means to drive defense business to U.S. contractors. This is true. By creating arms races and supplying prestige weapons, however useless, to unstable areas of the world, they are creating U.S. jobs. But wouldn’t taxpayer money and efforts be better spent if officials more precisely targeted domestic concerns with taxpayer funds rather than hoping that efforts trickle down predictably from collaboration with corpulent and unsavory foreign generals?

In the land of perverse incentives, SC funding is one of the most egregious—and in the post-9/11 era, many officials see SC as a critical tool of strategic positioning. However, the premises of SC must be reconsidered before the U.S. military squanders more resources on white elephant projects.

#### Mission creep supercharges the link – plan’s NATO-specific authorization will be stretched by non-NATO planners who game the system

Thaler 16 David E. Thaler, Senior International/Defense Researcher at RAND, MIA International Security Policy/Middle East, Columbia University; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Beth Grill, Senior Policy Analyst at RAND, MA Middle Eastern Studies and Economics, Johns Hopkins University School of Advanced International Studies; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; and Amanda Kadlec, RAND; “From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation,” RR1438, RAND Corporation, 2016, https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1400/RR1438/RAND\_RR1438.pdf /GoGreen!

Similarly, authorities that restrict activities to specific mission areas are seen as inflexible in the face of quickly emerging threats, making it difficult to build partner capacity in intended mission areas and further impelling SC personnel to “game” the system to achieve their SC objectives. After 2001 and until recently, the priority for U.S. national security strategy and for SC (and DoD activity in particular) has been counterterrorism.24 Congress established Section 1206 and many other recent SC authorities on the basis of the need to rapidly respond (and help partners respond) to threats from al-Qaeda and more recently the Islamic State of Iraq and the Levant (ISIL). But as the CT mission area has been addressed in the past ten to 15 years, other missions have emerged that are becoming priorities for the United States and its partners but that are not explicitly covered under the CT rubric (or under “stability operations,” another area addressed in authorities). These other emerging areas include cyber warfare and “hybrid” warfare of the type Russia has utilized to subjugate eastern Ukraine and annex Crimea (gaps are also addressed in a subsequent section of this chapter). Capstone DoD strategic planning guidance that defines priorities and directs the efforts of the CCMDs also identifies nontraditional threats, such as transnational border security, maritime security, and foreign fighters.25 While Congress and the administration have created some specific programs to bolster Ukraine and eastern NATO allies,26 existing authorities do not provide the flexibility for SC personnel to pursue these mission areas in other nations or regions. Thus, they are left with “stretching” existing authorities to achieve key objectives with partners.27

### AT: N/L – Plan Funds

#### Funding is NOT normal means

Thaler 16 David E. Thaler, Senior International/Defense Researcher at RAND, MIA International Security Policy/Middle East, Columbia University; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Beth Grill, Senior Policy Analyst at RAND, MA Middle Eastern Studies and Economics, Johns Hopkins University School of Advanced International Studies; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; and Amanda Kadlec, RAND; “From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation,” RR1438, RAND Corporation, 2016, https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1400/RR1438/RAND\_RR1438.pdf /GoGreen!

A second general area of concern for DoD’s SC workforce relates to the unpredictability in Title 10 SC funding to enable planning of initiatives and activities and the constraints on application of funds in execution. Many DoD discussants indicated that the DoD strategic planning guidance mandates a five-year planning horizon, yet Title 10 funding is available in much-shorter–term one- or two-year increments. This injects an enormous amount of “guess-work”—according to one discussant, “We are always gaming, guessing how much we think we are going to get”34—into planning and limits predictability and flexibility.35 According to another, “the Department lacks the ability to engage in long-term activities with partner nations…. Programs are episodic, and are generally not sustainable.”36 This has had deleterious effects in a number of ways.

First, the Theater Campaign Plans (TCPs) that guide SC, operations, posture, and other activities within a CCMD often are approved despite lack of insight into whether the programs to achieve TCP objectives will be available.37 Strategic guidance mandates that DoD components develop five-year plans and identify how they intend to achieve their theater objectives in that time. But these DoD components do not know how much funding they will receive for SC under Title 10 beyond one or two years and can only speculate on what is possible in the third, fourth, and fifth years. For example, Section 1203, a relatively new authority that allows U.S. general purpose forces (GPF) to train with partner GPF (in a manner akin to the well-regarded JCET program for SOF), is intended to enable training of U.S. forces while furthering partnerships with foreign military forces. Yet it does not come with funding, and must compete for O&M funds that are sorely needed elsewhere, including for operational readiness of U.S. forces.38 Representatives from a number of CCMDs have said they do not use Section 1203 or, if they do, only rarely. With no funding, it is difficult to assume it can be used in planning one year, much less five years, hence.

### AT: N/L – Budget Space

#### No budget space

Kelly 10 Terrence K. Kelly, principal mathematician at the RAND Corporation, former director of the RAND Homeland Security Research Division, formerly served for 20 years as a commissioned officer in the U.S. Army, positions included senior national security officer in the White House Office of Science and Technology Policy, PhD mathematics, Rensselaer Polytechnic Institute; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; Cathryn Quantic Thurston, Political Scientist at RAND, PhD Conflict Analysis and Resolution, George Mason University; Jennifer D. P. Moroney, senior political scientist at RAND, PhD international relations, University of Kent at Canterbury; and Charlotte Lynch, researcher at RAND; “Security Cooperation Organizations in the Country Team Options for Success,” RAND Corporation, 2010, <https://apps.dtic.mil/sti/pdfs/ADA517323.pdf> /GoGreen!

Current world conditions both create significant demands for U.S. security cooperation programs and deplete available resources to carry out these missions. The wars in Iraq and Afghanistan are occupying the regular, reserve, National Guard, and Special Forces trainers and advisors who would normally be called on to train and advise military counterparts. Furthermore, U.S. allies, who often complement the efforts of U.S. advisors and trainers, are also stretched thin by their own deployments to Iraq and Afghanistan.

#### That’s the whole point of AM&E

Hooper 17 Lieutenant General Charles W. Hooper, US Army, Director, Defense Security Cooperation Agency, Senior Research Fellow at the Weatherhead Center for International Affairs, Harvard University, MPA Harvard University, graduate of the graduate of the U.S. Army War College and United States Military Academy at West Point, “Managing Security Assistance To Support Foreign Policy,” prepared statement before the Committee on Foreign Relations, U.S. Senate, 9-26-2017, <https://www.govinfo.gov/content/pkg/CHRG-115shrg37504/html/CHRG-115shrg37504.htm> /GoGreen!

To address these challenges, the Deputy Assistant Secretary of Defense for Security Cooperation has focused on improving the planning, prioritization, and synchronization of Title 10 programs. These efforts have effectively postured the SC community to address the significant reforms laid out in the FY 2017 NDAA.The FY 2017 NDAA identified SC as a core DoD mission by establishing a new chapter of Title 10. This new SC chapter is meant to enhance flexibility, transparency, oversight, and management of programs and resources; professionalize the SC workforce; and improve the alignment of SC activities with defense strategy. These new authorities provide DoD a unique opportunity to transform SC into a more strategic U.S. national security tool.

Specifically, the FY 2017 NDAA:

consolidates policy oversight and resource allocation within the Office of the Secretary of Defense and consolidates execution and administration of Title 10 Security Cooperation programs within DSCA;

requires the DoD to provide a consolidated budget justification and establish an Assessment, Monitoring and Evaluation (AM&E) framework to allow a more rigorous, data-driven assessment of program effectiveness; and

mandates the DoD establish a SC workforce development program to ensure that the SC professionals all over the world have the appropriate training, education and experience to execute the mission.

Comprehensive SC Reform Implementation

Together with the Office of the Under Secretary of Defense for Policy, the Joint Staff, and the DoS, DSCA has developed an operational approach with four focus areas to implement SC reform mandated by the FY 2017 NDAA and to incorporate the Title 22 initiatives already underway. These focus areas, with the broad participation and support of the interagency, are designed to advance innovative policies and processes to address the following issues:

Governance and Oversight to oversee SC efforts and ensure compliance with legislative and policy requirements;

Policy Guidance to develop and issue policy to provide overarching direction for implementation of SC activities;

Execution to define and implement changes to SC capabilities and operations; and

Enabling Functions to perform operations required to support the execution activities.

Work on SC reform is well underway to meet current challenges and the requirements set forth in the FY 2017 NDAA.

Conclusion

Now more than ever, policy makers use SC as a critical tool to achieve our defense and foreign policy objectives. With reduced U.S. force structure and finite resources in a dynamic, rapidly evolving environment, it has become increasingly important to optimize allies' and partners' contributions to their own security and, by extension, U.S. security. The language in the FY 2017 NDAA provides the mandate to realize much needed reform to SC.

For the last 70 years Security Cooperation has been a pillar of U.S. foreign policy. We must not, however, rest on our laurels. Today, the convergence of Congressional mandates with the Department's emphasis on strengthening our partners is a call to action. We must seize this opportunity to fortify our status as the Security Cooperation partner of choice.

#### Resources are finite

Harvey 17 Thomas H. Harvey III, Acting Assistant Secretary of Defense for Strategy, Plans, and Capabilities, Office of the Secretary of Defense, U.S. Department of Defense, “Managing Security Assistance To Support Foreign Policy,” statement before the Committee on Foreign Relations, U.S. Senate, 9-26-2017, <https://www.govinfo.gov/content/pkg/CHRG-115shrg37504/html/CHRG-115shrg37504.htm> /GoGreen!

Most DoD security assistance programs are bounded by statutory obligations to jointly develop and plan their activities in conjunction with the State Department and to secure Secretary of State concurrence before implementing them. The Department of Defense recognizes the importance, even the essential imperative, of conducting business in this way. In our government, no department has the luxury of pursuing uncoordinated efforts, especially given finite resources and growing threats. While it may not have always been so, I would venture to say that, currently, all DoD's security assistance programs are shaped and approved at some level, and often at multiple levels, by the State Department, from the country team to the regional function bureaus at main State, to the Secretary himself.

### AT: N/L – No Tradeoff

#### Structural limitations compound – scarce staffing and budgetary constraints, a spaghetti bowl of conflicting authorities, funding cycles, and reporting requirements, and high turnover ALL make tradeoffs in DoD planning unavoidable – they cannot walk and chew gum

Thaler 16 David E. Thaler, Senior International/Defense Researcher at RAND, MIA International Security Policy/Middle East, Columbia University; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Beth Grill, Senior Policy Analyst at RAND, MA Middle Eastern Studies and Economics, Johns Hopkins University School of Advanced International Studies; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; and Amanda Kadlec, RAND; “From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation,” RR1438, RAND Corporation, 2016, https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1400/RR1438/RAND\_RR1438.pdf /GoGreen!

First, the proliferation and complexity of authorities make it difficult to develop security cooperation initiatives with partners, especially ambitious efforts that integrate several types of activities requiring multiple authorities. Every authority details different requirements and constraints concerning which partners are eligible, under what circumstances, and with what reporting requirements. Military planners in the field often have little experience managing security cooperation and rotate every two to three years, while more experienced DoD civilians are few in number with perhaps a handful to support a combatant command. Many initiatives require several authorities using different sources of funding on different cycles with different processes and restrictions, and different congressional reporting requirements. Should funding for one of these authorities fall through, major events may be canceled or radically restructured. Despite its value in helping deploy partners to Afghanistan, the Coalition Readiness Support Program example discussed earlier provided only one of the five authorities necessary to support four infantry battalions from the country of Georgia. Similarly, it was one of only six authorities required to loan Mine Resistant Ambush Protected vehicles to another country. In addition to the inefficiencies created by this patchwork approach, the delays and changes that result from associated planning problems can generate confusion with partners and setbacks in strengthening relationships and building a partner’s capabilities. Even more-modest efforts can require multiple authorities, leading some planners to avoid smaller programs because they may only have time for one or two high-visibility efforts. Finally, greater complexity has required greater involvement by DoD lawyers to interpret what is and is not allowed, with different interpretations by different individuals or organizations or at different times. For example, can a particular maritime training event be considered a counterterrorism effort? Can a particular exercise pay for certain civilians to attend? Legal uncertainties like these have resulted in delays and cancellations, generating further frustration and confusion between U.S. and foreign military planners.

#### It’s NOT a one-shot deal – it’s an ongoing, ever-expanding commitment to thirty countries – planners perceive multiplicative, NOT just additive, opportunity costs

Gold 21 Zack Gold, Ralph Espach, Douglas Jackson, and Nicholas Bradford, researchers in the Strategy, Policy, and Plans division of the Center for Naval Analyses, where they have conducted numerous evaluations of security cooperation activities for the U.S. military in recent years, “A Better Way to Measure Returns on U.S. Security Cooperation Investments,” Defense One, 6-16-2021, <https://www.defenseone.com/ideas/2021/06/better-way-measure-returns-us-security-cooperation-investments/174742/> /GoGreen!

Second, even if the returns were quantifiable, the real costs of security cooperation for the U.S. military are often unmeasurable. For example, past analysis indicates that the structure of the Navy’s cost accounting system makes it impossible to know the full, exact cost of any security cooperation deployment or activity. Additionally, there is opportunity cost in every decision about security cooperation. In Washington, the focus in recent years has been on realigning resources for great power competition. However, each geographic combatant command has dozens of partners. How, for example, can one accurately calculate the real and opportunity costs of conducting a bilateral exercise with Brazil as opposed to Colombia; or even with the UAE navy versus the UAE armed forces?

Third, return on investment focuses on the wrong unit of analysis. By trying to quantify the costs and returns of isolated security cooperation activities, evaluations fail to capture the full context of security cooperation with U.S. partners. The U.S. conducts security cooperation as integrated, iterative, or mutually supporting activities that involve multiple countries or multiple elements of a single country. For example, providing a patrol craft, training a crew, and exercising patrol operations are all discrete security cooperation activities, but which is responsible for building a partner’s maritime patrol capability—and can any of these activities achieve that desired outcome without the others? The outcomes of these activities are therefore not an additive result of individual security cooperation activities, but oftentimes a multiplicative one, further reducing the utility of return on investment as a useful tool.

#### Mission creep supercharges the link – plan’s NATO-specific authorization will be stretched by non-NATO planners who game the system

Thaler 16 David E. Thaler, Senior International/Defense Researcher at RAND, MIA International Security Policy/Middle East, Columbia University; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Beth Grill, Senior Policy Analyst at RAND, MA Middle Eastern Studies and Economics, Johns Hopkins University School of Advanced International Studies; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; and Amanda Kadlec, RAND; “From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation,” RR1438, RAND Corporation, 2016, https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1400/RR1438/RAND\_RR1438.pdf /GoGreen!

Similarly, authorities that restrict activities to specific mission areas are seen as inflexible in the face of quickly emerging threats, making it difficult to build partner capacity in intended mission areas and further impelling SC personnel to “game” the system to achieve their SC objectives. After 2001 and until recently, the priority for U.S. national security strategy and for SC (and DoD activity in particular) has been counterterrorism.24 Congress established Section 1206 and many other recent SC authorities on the basis of the need to rapidly respond (and help partners respond) to threats from al-Qaeda and more recently the Islamic State of Iraq and the Levant (ISIL). But as the CT mission area has been addressed in the past ten to 15 years, other missions have emerged that are becoming priorities for the United States and its partners but that are not explicitly covered under the CT rubric (or under “stability operations,” another area addressed in authorities). These other emerging areas include cyber warfare and “hybrid” warfare of the type Russia has utilized to subjugate eastern Ukraine and annex Crimea (gaps are also addressed in a subsequent section of this chapter). Capstone DoD strategic planning guidance that defines priorities and directs the efforts of the CCMDs also identifies nontraditional threats, such as transnational border security, maritime security, and foreign fighters.25 While Congress and the administration have created some specific programs to bolster Ukraine and eastern NATO allies,26 existing authorities do not provide the flexibility for SC personnel to pursue these mission areas in other nations or regions. Thus, they are left with “stretching” existing authorities to achieve key objectives with partners.27

### AT: N/L – Compartmentalized

#### The disad’s NOT about overstretching the people publishing the studies, rather the people planning and implementing the programs that are supposed to be studied – those people do trade off

Dyekman 7 Gregory J. Dyekman, Colonel, U.S. Army, Chief of Effects Assessment and Targeting in the Strategic Operations Directorate, MultiNational Force Iraq, MSS Army War College, MS Management, Troy State University, “Security Cooperation: A Key to the Challenges of the 21st Century,” Strategic Studies Institute, November 2007, <https://publications.armywarcollege.edu/pubs/1916.pdf> /GoGreen!

COCOMs will also likely face continued challenges in finding sufficient resources in the form of military personnel to conduct security cooperation programs. The Joint Strategic Capabilities Plan (JSCP) does not apportion forces specifically for security cooperation, and they must come from forces assigned to a COCOM’s AOR or that temporarily deploy for engagement activities.40 For the foreseeable future, the deployment requirements to support the GWOT will continue to leave few opportunities for active and reserve component units to participate in coalition and multinational exercises. In struggling to meet its surge requirements in Iraq and Afghanistan, the U.S. military is falling short in its ability to resource the steady-state deterrence and partner enabling missions called for in the QDR strategy.41 To address this shortcoming, President George W. Bush’s 2008 budget contains proposed funding for an additional end-strength increase of 92,000 troops for the Army and Marine Corps by 2013.42 This increase is not only necessary now, but also is required post-Iraq/Afghanistan. The Army must be forthright and convincing with the nation’s civilian defense leadership about the future force structure required to meet the myriad of “Boots on the Ground” tasks necessitated by an uncertain and complex environment.43

### AT: N/L – Not AM&E

#### It’s the most likely to be deprioritized – at which point, the window of opportunity will close

Yayboke 19 Erol Yayboke, senior fellow with the International Security Program and director of the Project on Fragility and Mobility at the Center for Strategic and International Studies, teaches global fragility and resilience at the Maxwell School of Citizenship and Public Affairs at Syracuse University, MPA, BBA international business, University of Texas at Austin; MacKenzie Hammond, research associate at CSIS; Hijab Shah, research associate at CSIS; and Melissa Dalton, senior fellow and deputy director of the CSIS International Security Program; “Assessment, Monitoring, and Evaluation in Action for Security Sector Assistance,” Commentary, Center for Strategy and International Studies, 6-27-2019, <https://www.csis.org/analysis/assessment-monitoring-and-evaluation-action-security-sector-assistance> /GoGreen!

From the faltering of the Iraqi security forces in the face of the so-called Islamic State in 2014 to the current controversy surrounding U.S. arms sales to Saudi Arabia, U.S. security sector assistance (SSA) to allies and partners has undergone significant scrutiny and reform recently. Jumpstarted by the FY 2017 National Defense Authorization Act (NDAA), one focus area of the SSA reform effort has been assessment, monitoring, and evaluation (AM&E). Long a core component of international development programming, the push to institutionalize AM&E in SSA programming is a result of recent congressional and executive branch efforts to increase accountability, transparency, and empirically-driven planning and design into SSA in the pursuit of U.S. interests and values.

AM&E is perhaps the weakest link of the SSA reform effort, yet it is the area that could most effectively help the U.S. government measure the impact and return on investment of the billions of dollars spent on SSA programs. The SSA goals, however, are ambitious—coordinating AM&E efforts and lessons across cross-funded, multi-year, multi-sectoral programs to address national security and broader foreign policy objectives. With policy and lawmakers’ attention focused on improving SSA, there is a window of opportunity for the primary SSA program implementers, the Department of Defense (DoD) and Department of State (DoS), to leverage the lessons learned by the U.S. development community—including the U.S. Agency for International Development (USAID) alongside other private and non-governmental organizations—to critically examine and strengthen AM&E for SSA.

#### Short-term bias makes the most useful AM&E particularly likely to get deprioritized in the face of plan’s fiat of an urgent new priority

Dyekman 7 Gregory J. Dyekman, Colonel, U.S. Army, Chief of Effects Assessment and Targeting in the Strategic Operations Directorate, MultiNational Force Iraq, MSS Army War College, MS Management, Troy State University, “Security Cooperation: A Key to the Challenges of the 21st Century,” Strategic Studies Institute, November 2007, <https://publications.armywarcollege.edu/pubs/1916.pdf> /GoGreen!

Resource challenges to security cooperation derive from fiscal constraints, Operational Tempo (OPTEMPO), Global Force Posturing, and outdated authorities. From a fiscal standpoint, the strategic environment will make the task of addressing our security challenges problematic for the foreseeable future. DoD’s 2007 budget is projected to be 3.9 percent of gross domestic product (GDP). As a percentage of GDP, DoD outlays are historically low and have not kept pace with the growth of GDP over the last 40 years.31 However, the rising costs of mandatory government entitlement spending associated with Medicare, Medicaid, and Social Security are projected to account for 11 percent of the U.S. GDP by 2016 and will exert pressures on a budget that economic growth alone is unlikely to alleviate.32 Entitlement obligations will likely result in political pressure to further reduce defense discretionary spending in order to forestall greater budget deficits. Despite the constrained fiscal environment, DoD outlays must continue to grow to meet our global engagement requirements. This should be a continuous strategic communication message implemented by DoD senior leadership to Congress and the American people to counter a growing view that the federal government already spends too much on national defense.33

Despite having the authority to plan and conduct security cooperation within their area of responsibility (AOR), GCCs currently lack sufficient dedicated resources to support their security cooperation strategy. In addition, existing resources are limited by multiple and conflicting policy and legislation. Up to 30 sources of funding regulated by various authorities and guidelines are required to implement GCC security cooperation strategies.34 Security Assistance programs like international military education and training (IMET), foreign military financing (FMF), and financial management service (FMS) are State Department funded, and COCOMs have limited ability through the interagency process to influence where and how this money is spent.35 Other sources like Warsaw Initiative Funding (WIF) and Cooperative Threat Reduction (CTR) funding support military exercises and capacity building efforts but continue to come under increased program management scrutiny. In the past, security cooperation funding by Service Components has contributed significantly to COCOM plan execution. However, Service Chiefs face growing fiscal obligations. As an example, the Army delayed submitting its 2008-13 Program Objective Memorandum in an effort to avoid a QDR strategy and resource mismatch.36 A mismatch still exists, and the Army faces a growing problem in funding current equipment wartime reset requirements and its modernization efforts. In recent congressional testimony, the Army Chief of Staff outlined the Army equipment reset bill at $17.01 billion for FY 2007, with expected requirements beyond 2007 to be $12 to $13 billion per year though the conflict and a minimum of 2 to 3 years beyond.37 Additionally, the Army will need nearly $200 billion for the Future Combat System and its associated spin-off technologies to meet modernization requirements.38 These fiscal realities suggest Service components will have fewer resources to dedicate to security cooperation, as Service Chiefs, who already have less interest in engagement programs, struggle to meet their Title 10 responsibilities to train, organize, and equip their forces.39 To overcome these hurdles, funding streams must be consolidated and reforms initiated that provide GCCs more influence in the allocation of funding resources for security cooperation.

COCOMs will also likely face continued challenges in finding sufficient resources in the form of military personnel to conduct security cooperation programs. The Joint Strategic Capabilities Plan (JSCP) does not apportion forces specifically for security cooperation, and they must come from forces assigned to a COCOM’s AOR or that temporarily deploy for engagement activities.40 For the foreseeable future, the deployment requirements to support the GWOT will continue to leave few opportunities for active and reserve component units to participate in coalition and multinational exercises. In struggling to meet its surge requirements in Iraq and Afghanistan, the U.S. military is falling short in its ability to resource the steady-state deterrence and partner enabling missions called for in the QDR strategy.41 To address this shortcoming, President George W. Bush’s 2008 budget contains proposed funding for an additional end-strength increase of 92,000 troops for the Army and Marine Corps by 2013.42 This increase is not only necessary now, but also is required post-Iraq/Afghanistan. The Army must be forthright and convincing with the nation’s civilian defense leadership about the future force structure required to meet the myriad of “Boots on the Ground” tasks necessitated by an uncertain and complex environment.43

In the long term, the Realigned Global Force Posture aimed at creating a CONUS based expeditionary force could have negative consequences for future shaping activities. The Army has typically provided over 60 percent of the support to the GCC engagement efforts through its forward stationed forces.44 In Europe alone, Army restationing will reduce the forward presence in Europe to only two permanent Brigade Combat Teams. Potential GWOT commitments aside, this reduction in forward based forces will either reduce USEUCOM’s military exercise and training programs or significantly increase transportation costs for CONUS based force participation. Alleviating some of these issues will be the decision to rotate forces to Bulgaria and Romania. General John Craddock, the new Supreme Allied Commander Europe (SACEUR), views this as an opportunity to “focus on mil-to-mil activities that continue to build the military capacities of new NATO Alliance and perspective Alliance countries along with strategic partners in Eastern Europe and Eurasia.”45 However, to truly allow GCCs the predictable manning resources, TSCPs must be integrated into the Global Force Management construct. The Army Force Generation (ARFORGEN) model provides a great opportunity to make forces available for GCC security cooperation requirements.

Resource challenges are also found in the numerous policy, regulatory, and legislative constraints governing the execution of programs. In testimony before the House Armed Services Committee, SACEUR General James L. Jones said:

Although the threats we face have changed dramatically, resources available for security cooperation, one of our key enablers in dealing with present day challenges, are still used as they have been since the Cold War. They are applied for deliberate, long-lead-time system built to address a single, enduring and predictable enemy.46

An example of outdated resourcing can be found in the authorities enabling the military to train and equip partner nations. The GTEP, while eventually successful, required funding from seven different agencies and allied contributions delaying the program start by seven months.47 Most State Department funded security assistance programs like FMS require multiple years to be put in place. To overcome this, the Bush administration sought and received limited authority to train or equip other countries’ militaries to respond to critical needs and meet emergent threats and opportunities. Under a 2-year pilot program, Section 1206 of the National Defense Authorization Act for 2006 provided $200 million in authority for GCCs to build the capability of military forces of a foreign country to conduct counterterrorist operations or participate in or support stability operations.48 While a vast improvement, the amendment still lacks elements the DoD requested, and others desired. Key among these is the limitation on training only national military forces vice border security and other security forces engaged in counterterrorism and stability operations.49 In its Building Global Partnerships Act of 2007, DoD submitted legislation for congressional consideration to expand the type of forces that may be trained and increase the funding ceiling to $750 million while making the 1206 authority permanent.50 The Act also seeks legislative provisions to streamline the authorities to increase our partners’ capacities through logistical and material support. It contains requests for permanent authorities to loan significant military equipment to coalition partners participating in combined operations and to allow GCCs to make grants of nonlethal excess defense articles.51 These legislative proposals to increase authorities are critical to increasing our partners’ effectiveness and must be enacted, streamlined, and fully funded.

Another example of legislative constraints exists with the DoD Regional Centers. Legislatively, the centers are now able to fund only military and civilian defense officials. Expanding the participant pool would strengthen their ability to educate and network with those necessary to counter ideological support for terrorism. In Middle East societies, where religion is so deeply integrated, Imams with greater understanding of democratic principles and common security challenges could be influential with Muslim populations, thereby countering extremism. Strategic communications could be further enhanced if influential moderates with access to al-Jazzera were educated at the centers. Lacking authority to waive costs for a broader pool of participants, Regional Centers are unable to reach the influential audiences most critical to U.S. interests. In the uncertain and rapidly changing security environment we now face, we must not continue to embrace outdated models and antiquated mindsets in dealing with allies and partners. The flexibility offered by initiatives like partner capability and capacity building legislation in the Building Global Partnerships Act is a necessary start. To truly be effective, however, the United States must completely reexamine the Foreign Assistance Act and undertake broad reform of the ways in which we provide security assistance.

Another growing challenge to security cooperation lies in the necessity to properly assess and evaluate program effectiveness. In the domestic strategic environment of scarce and competing defense resources, it will be critical for COCOMs to evaluate their security cooperation programs to establish priorities, defend funding, and apply their resources where most needed. To date, the submission of engagement plans has simply served as a venue to capture and inform the Joint Staff of what the COCOMs are doing but fail to demonstrate their effectiveness.52 The 2005 Security Cooperation Guidance outlining the requirement to conduct an annual assessment of security cooperation activities in their AORs is a beginning. No assessment guidance has been published by DoD, however.

Historically, the subjective nature of security cooperation has made it very difficult to measure. Assessment has consisted mainly of capturing and reporting outputs, including details such as the number of exercises, students trained, and port calls have served as the measure of program success. Assessment templates should require addressing measures of performance, or how well a plan was executed and also how well programs are aligned with priorities for creating and building partnerships outlined in the Security Cooperation Guidance. To truly transform security cooperation effectiveness, however, one must address the difficult task of measuring effectiveness. Assessment plans should evaluate programs against broader cooperation efforts.53 COCOMs must begin to measure in terms of strategic outcomes, measuring the effectiveness of how well their plans build partners and capacity. The Building Partnership Capacity (BPC) Roadmap, signed in May 2006 by Deputy Defense Secretary Gordon England to provide a plan of action for implementing partnership capacity related QDR decisions, may prove constructive if it improves DoD’s ability to assess security cooperation investments.54

While properly measuring effectiveness is vitally important to prioritizing resources, caution must be taken to avoid a short-term focus. The emerging security environment may lead to a significant resource struggle to achieve a proper balance between short- and long-term programs with respect to measuring the effectiveness of attaining security cooperation objectives. A steady shift to more immediate, tangible, and measurable outcomes from theater security programs is likely. However, a business mindset towards assessments should not force policy practices to favor short term, metric oriented programs that have quick and measurable tactical effects. The difficulty of measuring security cooperation success creates problems when evaluating progress over time. Many long-term benefits in engagement programs that build partner will through trust and mutual understanding exceed the scope of any single program and progress more often comes from multiple programs conducted over many years.55 Ongoing multifaceted cooperation in the GWOT is an example where long-term U.S. military cooperation efforts have achieved valuable outcomes. In congressional testimony, USEUCOM Commander General Jones said:

Since September 11, 2001, nearly every nation in the USECUOM AOR has offered or provided intelligence, basing access, and over-flight rights, forces, and equipment as well as other forms of key support in our efforts to combat terrorism. The degree of support we have received is directly related to the effort and attention we have given to the security cooperation program that was in place well in advance of the current conflict.56

In the security environment of uncertainty the United States faces, long-term efforts to build and maintain a foundational base of security partners through exercises, military education, and exchanges are wise investments to hedge against future security challenges. Assessment constructs must capture both short- and long-term returns.

## UNIQUENESS

### AT: U O/W – Requirements

#### It’s NOT inevitable – despite legal requirements

Walther-Puri 21 Andrea Walther-Puri, PhD candidate, Fletcher School of Law and Diplomacy, research focuses on the effects of U.S. military counterterrorism programs on longer-term security governance transformation in the Sahel, “Afghanistan: A Tragic Lesson of the US Military’s Flawed Approach to Capacity Building,” Just Security, 9-6-2021, <https://www.justsecurity.org/78086/afghanistan-a-tragic-lesson-of-the-us-militarys-flawed-approach-to-capacity-building/> /GoGreen!

There were many flaws in the way the United States measured the effectiveness of its efforts. While the U.S. Defense Department (DOD) is required by law to conduct assessment, monitoring, and evaluation of its capacity building programs, whether this is carried out and the quality of those efforts is not always guaranteed. Standardized methods to measure results did not exist in Afghanistan. During the 20-year effort, operational assessments from top U.S. military leaders exhibited entrenched optimism, which “bore no resemblance” to conditions on the ground.

#### The pace of implementation is everything – the whole problem’s that checking the math is hard and resource-intensive so gets repeatedly deprioritized in the face of more immediate demands on planners – which means link controls uniqueness – plus, there’s no sufficiently fast threshold for which we can be certain of beating competitors, it’s a relative, NOT absolute question

Yayboke 19 Erol Yayboke, senior fellow with the International Security Program and director of the Project on Fragility and Mobility at the Center for Strategic and International Studies, teaches global fragility and resilience at the Maxwell School of Citizenship and Public Affairs at Syracuse University, MPA, BBA international business, University of Texas at Austin; MacKenzie Hammond, research associate at CSIS; Hijab Shah, research associate at CSIS; and Melissa Dalton, senior fellow and deputy director of the CSIS International Security Program; “Assessment, Monitoring, and Evaluation in Action for Security Sector Assistance,” Commentary, Center for Strategy and International Studies, 6-27-2019, <https://www.csis.org/analysis/assessment-monitoring-and-evaluation-action-security-sector-assistance> /GoGreen!

Although elements of DoD and DoS have begun to incorporate AM&E into their SSA programming after recent policy changes—examples being the 2017 DoD Instruction 5132.14: Assessment, Monitoring and Evaluation Policy for the Security Cooperation Enterprise, as well as DoS’ 2016 Program and Project Design, Monitoring and Evaluation Policy and the Foreign Aid Transparency and Accountability Act —these efforts are nascent and could benefit significantly from lessons learned from the development community including monitoring and evaluation frameworks, data collection methodologies, and feedback mechanisms.

Adapting traditional AM&E from the development community for SSA programming will not only require closer interagency coordination and dialogue around best practices but will also necessitate significant skill building and workforce development. These practices include shared fluency in the various roles, authorities, and capabilities that currently exist in the interagency around AM&E-type activities; iterative processes that build in adaptability and flexibility to change and improve as the environment necessitates; and a common lexicon around AM&E that DoD, DoS, and USAID can all leverage as they seek to coordinate AM&E in SSA programming.

AM&E is heavily dependent on data collection and synthesizing information. While DoD and DoS collect a broad array of data for SSA programming purposes, it is often inconsistent, incomplete, and difficult to share across agency lines. These issues are exacerbated by the complex realities often found in SSA country contexts. To mitigate such issues, the SSA community can learn from and leverage existing development models to design programs using multi-step data collection processes that incorporate cross- and multi-sectoral data to gather context specific data, such as environmental challenges, political environment, or gender-related issues. Doing so effectively will require SSA policymakers and practitioners to prioritize AM&E starting from the design and planning stages, not as an afterthought to action.

#### Implementation is NOT inevitable

Marquis 16 Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; S. Rebecca Zimmerman, Policy Researcher at RAND; Merrie Archer, Senior Pol-Mil Policy & Plans Advisor, Bureau of Political Military Affairs, U.S. Department of State, MA International Affairs, Economic and Political Development, Columbia University; Jeremy Boback, assistant policy researcher at RAND; and David Stebbins, senior policy analyst at RAND; “Developing an Assessment, Monitoring, and Evaluation Framework for U.S. Department of Defense Security Cooperation,” RR1611, RAND Corporation, 2016, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1611/RAND_RR1611.pdf> /GoGreen!

At a time when the United States is increasingly relying on foreign partners for its security and attempting to build their military capacity, security cooperation activities and expenditures can no longer be justified with anecdotal evidence. In order to gauge security cooperation’s “return on investment,” senior leaders in the presidential administration and Congress are requesting a rigorous accounting of what is being done, what is being spent, and what is being achieved and not being achieved in relation to specific planning objectives across the security cooperation enterprise. Although many parts of the U.S. Department of Defense (DoD) already conduct some form of security cooperation–related assessments, monitoring, and/or evaluation, understanding and implementation vary widely. Without high-level DoD leadership, these efforts will likely remain ad hoc and difficult to regularize and aggregate in a manner useful for planning and management at various levels of DoD or for coordination and collaboration with security assistance sector partners outside the department.

#### O’Mahony concludes policy is NOT sufficient to ensure implementation

O’Mahony 18 Angela O’Mahony, associate dean for academic affairs at Pardee RAND Graduate School and a senior political scientist at RAND, former assistant professor of international political economy and economic statecraft at the University of British Columbia, PhD political science, UCSD; Ilana Blum, researcher at RAND; Gabriela Armenta, researcher at RAND; Nicholas Burger, senior economist at RAND and director of RAND’s Washington office; Joshua Mendelsohn, researcher at RAND; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Steven W. Popper, researcher at RAND; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; and Thomas S. Szayna, senior political scientist and former director of RAND's Defense and Political Sciences Department at RAND, MA international relations, Claremont Graduate School; “Assessing, Monitoring, and Evaluating Army Security Cooperation: A Framework for Implementation,” RR2165, RAND Corporation, 2018, <https://apps.dtic.mil/sti/pdfs/AD1056354.pdf> /GoGreen!

CHAPTER EIGHT

Conclusion

As security cooperation continues to be an important instrument for the Army to achieve its objectives, the Army needs a better understanding of relative effectiveness. Part I of this report found that recent Army security cooperation activities have aligned fairly well with what previous analyses have found contribute to effectiveness in both security cooperation and international development assistance. However, the lack of systematic AM&E across Army security cooperation activities has made it impossible to examine individual and aggregated activities in a way that truly drives prioritization efforts. This reflects both the inherent challenges that exist in evaluating security cooperation and the lack of robust AM&E processes throughout the Army and DoD more broadly.

OSD has worked to improve DoD enterprise-wide security cooperation AM&E procedures. Its recently released DoDI has enumerated requirements that are in keeping with good practices adopted by international development organizations and recognize the complexity of U.S. security cooperation in toto.1 However, OSD’s focus has been at the policy level and its guidelines serve primarily to provide guidance for GCC planners.

To help the Army better plan and execute its security cooperation activities, we developed AM&E implementation guidelines based on emerging OSD guidance, current Army processes, and good practices adopted by international development organizations. We expect the primary users of this framework and portfolio tool will be ASCC planners, while HQDA staff can use it in their oversight role. ASCC planners serve as the primary interface between GCCs, the department of the Army, and Army implementers. We believe that adopting the Army security cooperation AM&E framework presented in this report will provide a good foundation for deepening the Army’s understanding of its security cooperation effectiveness.

The Army’s focus on deepening its security cooperation AM&E procedures at the activity level can serve as a model for how DoD links its strategic guidelines to operational planning. The Army’s bottom-up operational approach can be a valuable complement for OSD’s top-down strategic approach, particularly with the help of the framework and portfolio tool developed in this report. Taken together, the OSD and Army approaches form the basis for a comprehensive process that accounts for strategic, operational, and tactical considerations in support of decisionmaking.

### AT: N/U – Deprioritized

#### NATO planners specifically are prioritizing AM&E

White House 21 The White House, “United States Strategy On Countering Corruption,” December 2021, <https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption-1.pdf> /GoGreen!

Building accountable, effective, and resilient security institutions: The United States, led by the Department of Defense (DOD), will work towards elevating, prioritizing, and surging funds to institutional capacity building (ICB) activities to leverage DOD’s significant history of, and expertise in, improving resiliency through support of democracy and anti-corruption efforts with our global partners. DOD’s ICB efforts, which also align with NATO’s Building Integrity program, are particularly well-placed to simultaneously integrate key principles of advancing democratic civil-military relations, building transparent and resilient security sectors, and strengthening civilian leadership across multiple institutional functional areas. In addition to continued support to NATO’s Building Integrity program, DOD will coordinate with State and USAID and can adapt the approaches presently used in DOD ICB to apply them more comprehensively toward democratization and anti-corruption outcomes. This effort will nest with DOD’s assessment, monitoring, and evaluation framework, as required by the FY17 NDAA. It will also advance DOD’s use of learning agendas to create positive feedback loops and better identify new ways of establishing responsible defense governance and internal controls in order to help build more accountable, effective, and transparent defense institutions with partners.

#### Next year’s budget proposal proves

DoD 22 Office of the Secretary of Defense, U.S. Department of Defense, “Fiscal Year (FY) 2023 President’s Budget Justification for Security Cooperation Program and Activity Funding,” April 2022, <https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Security_Cooperation_Justification_Book.pdf> /GoGreen!

The Department has made significant reforms to align strategic guidance with resource allocation; establish an assessment, monitoring, and evaluation (AM&E) program; and create a comprehensive, common picture of the Department’s budget for security cooperation activities as well as related programs that engage foreign partners. This budget display is a representation of the Department’s progress to date in achieving security cooperation reform and realizing congressional intent in Title 10, Chapter 16, security cooperation.

Section 381(a) of Title 10, U.S. Code, requires a consolidated budget of security cooperation programs and activities be included annually along with the President’s Budget request to Congress. The consolidated budget display is intended to enhance planning and oversight of security cooperation programs and related activities across the DoD. This annual budget display demonstrates how DoD plans, programs, and budgets for programs and activities to align with the Department’s strategic objectives.

This budget display includes the $3.7 billion requested by the Department for FY 2023 to conduct security cooperation programs and activities. It focuses primarily on the funding requested for programs and activities that will be executed under the authorities in Chapter 16 of Title 10, U.S. Code. It also includes funding requests for non-Chapter 16 programs and activities that include some elements or activities that are consistent with the security cooperation definition, including the Coalition Support Funds, the DoD Cooperative Threat Reduction (CTR) Program, Ukraine Security Assistance Initiative (USAI), and the Counter-Islamic State of Iraq and Syria (ISIS) Train and Equip Fund (CTEF). This display excludes classified programs, such as programs authorized under Section 127e of Title 10, U.S. Code, “support of special operations to combat terrorism.” The budget display also excludes Drug Interdiction and Counter-Drug activities authorized under Section 284(c) of Title 10, U.S. Code, “Support for counterdrug activities and activities to counter transnational organized crime.”

#### Implementation is gaining momentum

Pretelt 21 Maj. Carlos De Castro Pretelt, U.S. Army, Foreign Area Officer serving as the Operations Section Chief at the Office of Defense Coordination in Mexico City, MA International Policy and Practice, George Washington University, MA International Management, University of Phoenix, BS social psychology, Park University, “Taking a Bite out of the Elephant: How to Improve Security Cooperation,” Small Wars Journal, 7-17-2021, <https://smallwarsjournal.com/jrnl/art/taking-bite-out-elephant-how-improve-security-cooperation> /GoGreen!

In 2017, Congress sought to address this conundrum through the National Defense Authorization Act (NDAA). The NDAA directed the Secretary of Defense to implement an Assessment, Monitoring, and Evaluation (AM&E) framework to improve the accountability of all security cooperation initiatives; something akin to what PM/SA had been working on since 2015.[v] In theory, all security cooperation initiatives should be assessed to ensure USG funds are being used to advance or achieve a specific, measurable, achievable, relevant, and time-bound (SMART) objective that ultimately benefit US interests.[vi] It has been a number of years since the release of the NDAA, but this mandate is finally creating substantial ripples across the security cooperation community.

#### Capacity and processes are expanding

Stroul 21 Dana Stroul, Deputy Assistant Secretary of Defense for the Middle East, Office of the Secretary of Defense, U.S. Department of Defense, “U.S. Security Assistance In The Middle East,” prepared statement before the Subcommittee on Near East, South Asia, Central Asia and Counterterrorism, Committee on Foreign Relations, U.S. Senate, 8-10-2021, <https://www.foreign.senate.gov/imo/media/doc/08%2010%2021%20U.S.%20Security%20Assistant%20in%20the%20Middle%20East.pdf> /GoGreen!

The Department conducts assessment, monitoring, and evaluation (AM&E) of its security cooperation initiatives to inform decisions about security cooperation strategy, policy, programs, and resources. The Department is building its capacity and processes to design, develop, and implement AM&E to track progress through the development of front-end assessments and performance monitoring of security cooperation initiatives. In addition, the Department conducts independent strategic evaluations to analyze the efficiency and effectiveness of SC programming.

### AT: Thumper – Generic

#### No thumpers – all SC (other than Ukraine) is budgeted and planned far in advance – only plan’s fiat forces an unplanned reprioritization, which is what forces cancellations beyond the squo

Buell 18 Commander William A. Buell, US Navy, Branch Chief for Campaign Planning at Headquarters, U.S. Southern Command J5; Major Erin Dorrance, US Air Force, Military Deputy Chief in the Office of Congressional Affairs at U.S. Southern Command; and Robert West, Supply and Services Branch Chief at U.S. Southern Command J4; “Transregional Capstone Exercise Training for Tomorrow’s Fight,” Joint Forces Quarterly, iss.90, 2018, <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-90/jfq-90.pdf> /GoGreen! **\*\*to be clear, I am drawing some of the warrants from sentences that are “straw person” descriptions of objections DoD would make to a new SC activity – but they are portions the author explicitly agrees with, and I’ve boxed phrases like “this is true” and “indeed” to demonstrate that – the author is not disagreeing with these warrants as descriptions of the status quo, only suggesting how the reforms they advocate would change that – I believe the arguments I’m using this evidence to support are necessary and not merely plausible inferences**

Challenges

Too Hard to Integrate with Existing Exercises. Some may say a biennial exercise that includes all GCCMDs and FCCMDs is unrealistic given the often frantic operations tempo and fiscal constraints that burden DOD. At present, this is true. However, reevaluating existing exercises and either canceling or integrating them into the capstone exercise could alleviate much of the additional burden of a new mandatory requirement for the Joint Staff and CCMDs. Development of a TCE should follow the lessons learned from the North Atlantic Treaty Organization (NATO). In the wake of the Crimea crisis, NATO quickly went from about 100 to 300 exercises per year and reached the limit of the Allies’ ability to support them. Instead of adding additional exercises, NATO is now focused on increasing their realism, flexibility, and robustness. This change in thinking has allowed for NATO to plan and execute faster.19 Likewise, a TCE provides an opportunity for combatant commanders to set aside redundant training exercises while keeping the intent of higher guidance providing a “less-is-more” training option for the CCMD.

The first full biennial capstone exercise should not be executed until 2020 to provide planners adequate lead time to plan and schedule the exercise across DOD. Furthermore, a TCE would have to be assigned priority event status to ensure prioritization throughout DOD. Once scheduled far in advance, planners should be able to schedule other events around an established battle rhythm that runs a TCE every other year, on even years, starting in 2020.

Scheduling and Resources. Others might argue that a TCE is just another exercise requirement that takes away time they could spend on real-world issues and that there is not enough time and resources to do both. DOD and other agencies are indeed faced with fiscal challenges that have resulted in the United States having the smallest Army, Navy, and Air Force since World War II.20 At the same time, with the plethora of exercises already being executed, finding a time that would work across the joint force would be difficult. To address this concern, the Joint Staff and CCMDs should first establish a culture that recognizes the value of a TCE and set it as a top training priority in order to solidify support for aggressive exercise participation. Rotating through the five key challenges in a variety of scenarios could further validate the legitimacy of the exercise, as it would allow assigned CCMDs synchronizing responsibilities to exercise against a variety of benchmark threats. Despite the resource challenges, ensuring the Secretary, Joint Staff, and all GCCMDs and FCCMDs participate in the exercise is central to achieving proposed training objectives, especially command and control and communications stress-testing. Each GCCMD and FCCMD’s unique capabilities and geographic expertise should be represented in the exercise, and this would indeed pose the greatest challenge to scheduling and execution.

To address the resourcing issue, it is important to put a mark on the calendar as soon as possible to enable Global Force Management processes time to allocate any shift in resources. The Joint Staff and CCMDs will also need to quickly determine required staff to serve as role players and determine how best to meet this need. Options for building the necessary training elements could include assigning select staff a temporary duty assignment, employing modular training teams, hiring short-term contractors, or creating computer system simulations. For an exercise of this scale, new collaboration mechanisms among training elements might be required, as physical space to house a training element of this magnitude would likely not permit complete collocation. The key to addressing all of these challenges would be sufficient time for planning.

### AT: Thumper – Ukraine

#### Ukraine’s priced in – literally – next year’s budget proposal proves it has a separate account that does NOT pull from the general account that funds AM&E

DoD 22 Office of the Secretary of Defense, U.S. Department of Defense, “Fiscal Year (FY) 2023 President’s Budget Justification for Security Cooperation Program and Activity Funding,” April 2022, <https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Security_Cooperation_Justification_Book.pdf> /GoGreen!

INTERNATIONAL SECURITY COOPERATION PROGRAMS ACCOUNT:

The International Security Cooperation Programs (ISCP) Account funds activities aimed at building partner capacity to address shared national security challenges and operate in tandem with or in lieu of U.S. forces. These efforts include train-and-equip programs to build partner capability across a range of mission areas and institutional capacity building to facilitate absorption, sustainment, and institutional support necessary for capability development. Beginning in FY 2022, all Institutional Capacity Building (ICB) programmatic activities previously funded out of the Institute for Security Governance (ISG) and Institute of International Legal Studies (DIILS) accounts are funded out of the ISCP Account. The Department plans to use ISCP Account funds for activities under section 332 ICB, section 333 (Train-and-Equip), and P.L. 114-92 section 1263 (Indo-Pacific Maritime Security Initiative).

Security cooperation programs funded through the ISCP Account are prioritized across a range of factors, including strategic alignment, program feasibility, and DoD component prioritization. Geographic Combatant Commands develop and submit requirements in the form of significant security cooperation initiatives (SSCI), aligning proposed activities across five-year plans and identifying complementary Department of State security sector assistance activities (e.g., exercises, Foreign Military Financing, Foreign Military Sales, etc.) that contribute to the effort’s strategic objective. Initiative-based planning supports DoD’s efforts to conduct assessment, monitoring, and evaluation of security cooperation activities to ensure programs yield a return on investment. ISCP programs and activities are coordinated, reviewed, and vetted by the Secretary of Defense and the Secretary of State, facilitating synchronization of security sector assistance.

**[TABLE OMITTED]**

UKRAINE SECURITY ASSISTANCE INITIATIVE:

The Ukraine Security Assistance Initiative (USAI) will continue to build Ukraine's capacity to defend its sovereignty and territorial integrity. This funding provides assistance and support to the military and national security forces of Ukraine, and to other forces or groups recognized by and under the authority of the Government of Ukraine, including governmental entities within Ukraine, engaged in resisting Russian aggression. USAI also funds the replacement of any weapons or defensive articles provided to the Government of Ukraine from the inventory of the U.S.

In coordination with the Department of State, the initiative supports a variety of security assistance activities including, but not limited to: Intelligence support, personnel training, equipment and logistics support, supplies and other services. Specifically, this initiative is intended to enhance Ukraine’s capabilities to defend against Russian aggression, assist Ukraine in developing the combat capability to defend its sovereignty and territorial integrity, and support Ukraine’s efforts to effectively defend its sovereign territory against invading Russian forces.

**[TABLE OMITTED]**

#### Even “unexpected” increases are priced in – AND the Ukraine account still has more to give

Psaki 22 Jen Psaki, White House Press Secretary, “Press Briefing by Press Secretary Jen Psaki,” 4-20-2022, <https://www.presidency.ucsb.edu/documents/press-briefing-press-secretary-jen-psaki-149> /GoGreen!

Q: And on an unexpected announcement of another round of assistance to Ukraine, could you walk us through any specifics, if you have any, on that and when that's happening?

And just big picture on this: The U.S. has already given more than $2.5 billion since this war started. How long can the U.S. expect to continue to bankroll so much of this war?

MS. PSAKI: Well, okay, there's a couple questions there, so let me do my best in answering them.

First, we are working, of course, around the clock, as you know, to provide security assistance to Ukraine. And just to give you an example of how that assistance has flowed, just in the last few days -- and I think I gave an update the other day -- but five flights with military assistance have arrived in the region over the last few days. More than half a dozen flights from the United States are scheduled to land in the region shortly with additional equipment.

And as we look at providing this assistance, which I know -- I'll go back to the first part of your question, of course -- but what we've tried to do -- we made a strategic decision given we've seen Russia reposition their troops and their military to the eastern part of Ukraine to fight a different kind of war on the ground, which will be more, you know, kind of shooting back and forth through long range.

And so, we have been working with Ukrainians and the Ukrainian military to determine exactly the kind of security assistance they need for this stage in the war. And that has included an increase, as you've seen, in artillery and ammunition and weapons, like Howitzers and others, that can do these sorts of -- they can -- are effective in this long-range shooting and long-range fighting that we are seeing or we anticipate will happen in this stage of the war.

So, we have been expediting this assistance to the ground over the last couple of weeks to ensure they are prepared as this -- as this portion of the war is starting -- not because they are using all of it in in seven days, but because we want them to have all of this equipment as quickly as possible as they prepare to fight this war on the ground.

In terms of assistance and what we will be -- what we're preparing or the reports that I know have been out there, I will say I expect we'll have more soon on this, but I have nothing to preview at this point in time.

I would note that out of the $3.5 billion in drawdown authority Congress granted for this fiscal year, we've used over $2.4 billion so far to provide Ukraine the military equipment and capabilities they need to defend themselves.

So, obviously, there's more of that approved drawdown assistance that we can provide. And we've been working to expedite and ensure, as I noted, that it's meeting exactly the needs they have at this point in the war.

#### Most of the stuff their ev’s about comes from DoS assistance, NOT DoD cooperation – AND Congress has been adding supplemental funding specific to Ukraine to cover it all regardless

CRS 22 Congressional Research Service, “U.S. Security Assistance to Ukraine,” IF12040 version 9, CRS In Focus, updated 6-6-2022, <https://crsreports.congress.gov/product/pdf/IF/IF12040> /GoGreen!

The United States has been a leading provider of security assistance to Ukraine, both before and after Russia renewed its invasion of Ukraine on February 24, 2022. From 2014, when Russia first invaded Ukraine, through June 1, 2022, the United States has provided more than $7.3 billion in security assistance “to help Ukraine preserve its territorial integrity, secure its borders, and improve interoperability with NATO.” Since the start of the 2022 war, the Biden Administration has committed a total of more than $4.6 billion in security assistance to “provide Ukraine the equipment it needs to defend itself.”

FY2022 security assistance packages are being funded via more than $23 billion in regular and supplemental appropriations, including the Ukraine Supplemental Appropriations Act, 2022 (P.L. 117-103, Division N), and the Additional Ukraine Supplemental Appropriations Act, 2022 (P.L. 117-128). In total, FY2022 appropriations include $12.55 billion to replenish Department of Defense (DOD) equipment stocks sent to Ukraine via presidential drawdown authority; $6.3 billion for DOD’s Ukraine Security Assistance Initiative (USAI); and $4.65 billion in Foreign Military Financing (FMF) for Ukraine and “countries impacted by the situation in Ukraine.” FY2022 supplemental appropriations also have included funds for additional U.S. troop deployments to Europe.

Overview of Programs Since 2014

The United States has used a variety of security assistance programs and authorities to help build the defensive capacity of the Ukrainian Armed Forces (UAF) through train, equip, and advise efforts across multiple spending accounts. Prior to the 2022 war, the two primary accounts were the State Department’s FMF (22 U.S.C. §2763) and DOD’s USAI (P.L. 114-92, §1250) (see Table 2).

USAI packages have included training, equipment, and advisory efforts to enhance Ukraine’s defensive capabilities. FY2022 appropriations also directed that USAI funds be provided for logistics support, supplies, and services; salaries and stipends; sustainment; weapons replacement; and intelligence support. Prior to FY2022, a portion of annual USAI funds was contingent on DOD and State certifying Ukraine’s progress on key defense reforms.

The United States also has been providing defense items to Ukraine via Presidential Drawdown Authority (PDA), by which the President can authorize the immediate transfer of articles and services from U.S. stocks without congressional approval in response to an “unforeseen emergency” (22 U.S.C. §2318(a)(1)). Since August 2021, the Biden Administration has authorized 11 drawdowns valued at $4.26 billion (see Table 1).

Table 1. Presidential Drawdowns for Ukraine,

FY2021-FY2022

# Date Authorized Amount

1 August 27, 2021 $60,000,000

2 December 28, 2021 $200,000,000

3 February 25, 2022 $350,000,000

4 March 12, 2022 $200,000,000

5 March 16, 2022 $800,000,000

6 April 5, 2022 $100,000,000

7 April 13, 2022 $800,000,000

8 April 21, 2022 $800,000,000

9 May 6, 2022 $150,000,000

10 May 19, 2022 $100,000,000

11 June 1, 2022 $700,000,000

Total $4,260,000,000

Source: Department of State and Department of Defense.

Ukraine also has received assistance pursuant to DOD’s security cooperation authorities, notably Building Partner Capacity (10 U.S.C. §333) and Defense Institution Building (10 U.S.C. §332), and International Military Education and Training (IMET), which has provided professional military education at U.S. defense institutions for Ukrainian military officers. Other State Department- and DOD-funded security assistance has supported conventional weapons destruction, border security, law enforcement training, and counterweapons of mass destruction capabilities.

#### Ukraine is special, Congress will re-up as soon as it runs out – unlike small programs like AM&E

Kheel 5-19-22 Rebecca Kheel, congressional reporter for Military.com, former defense reporter for The Hill, BA newspaper journalism and history, Syracuse University, “Pentagon Can Ship More Weapons to Ukraine After Congress Replenishes Aid Funding,” Yahoo! Finance, 5-19-2022, <https://finance.yahoo.com/news/pentagon-ship-more-weapons-ukraine-200010021.html> /GoGreen!

The Senate gave final approval Thursday on a multibillion-dollar bill that will extend the Pentagon's ability to ship weapons to Ukraine the same day arms funding was set to dry up.

The Senate voted 86-11 to approve $40 billion in security and humanitarian aid for Ukraine, including nearly $20 billion in Pentagon funding to send more weapons to the front lines of the three-month-old war with Russia and support U.S. troops stationed elsewhere in Europe. All the "no" votes came from Republicans.

The bill, which already passed the House, is expected to be quickly signed into law by President Joe Biden.

Biden administration officials had been warning they expected to exhaust all of the existing funding to send weapons to Ukraine by Thursday, potentially stalling the flow of arms amid fierce fighting in Ukraine's eastern Donbas region. The Pentagon said the shipments will now continue and could include new types of weapons, depending on what is requested by the Ukrainians.

"The future drawdown packages will probably, at least in terms of frequency, look a lot like what we've done in the past," Pentagon spokesman John Kirby said. "We now have some longer runway, and so we're going to meter these out appropriately so that Ukraine is getting what it needs in the fight that they're in, and that flight could change over time."

Shortly after the Senate's vote, the Pentagon announced it was using the last $100 million of the previously approved funding to send Ukraine another 18 howitzers, 18 tactical vehicles to tow the howitzers, three counter-artillery radars, and field equipment and spare parts.

The bill approved Thursday gives the Pentagon another $8.7 billion to replenish U.S. weapons stockpiles being sent to Ukraine, as well as $6 billion for the Ukraine Security Assistance Initiative, the program Congress created in 2016 to buy weapons for and help train the Ukrainian military.

Ahead of Thursday's vote, Senate Majority Leader Charles Schumer, D-N.Y., said the funding could help "make sure that the Ukrainians are victorious," an outcome that seemed far-fetched ahead of the invasion -- when U.S. intelligence was warning Kyiv could fall to the Russians in days -- but which lawmakers are increasingly saying should be the goal of U.S. support to Ukraine.

Since Russia invaded Ukraine on Feb. 24, the United States has committed to sending about $3.9 billion in weapons and other military equipment, including thousands of Javelin anti-tank missiles and Stinger anti-aircraft missiles, hundreds of Switchblade kamikaze drones, more than 100 howitzers and more.

The bill also has $3.9 billion for U.S. military operations in Europe, including "mission support, intelligence support, hardship pay for troops deployed to the region and equipment including a Patriot battery," according to a summary of the bill released by House Appropriations Committee Democrats.

Thursday's bill brings the total U.S. funding approved to bolster Ukraine during the war to more than $53 billion, about half of which has been for the Pentagon.

Congress butted up against the deadline to refresh funding despite broad bipartisan support and hopes for a Senate vote immediately after last week's House vote because of Sen. Rand Paul, R-Ky., who would not agree to bypass lengthy Senate procedures unless the bill included his amendment.

Paul wanted the bill to add language that would expand the role of an inspector general for Afghanistan to include overseeing the Ukraine funding. Senate leaders were willing to give him a vote on his amendment, but Paul wanted the underlying bill to be rewritten to include his proposal.

While Paul's proposal was not included, the bill approved Thursday does require the Defense Department inspector general to conduct oversight of the funding.

### AT: Thumper – Taiwan

#### Taiwan does NOT thump – it’s priced in – appropriated separately – and there’s a massive backlog anyway, so new stuff just goes to the bottom of the docket – plus, funding isn’t implicated until it’s cleared – unlike plan’s fiated change in priorities

Harris 22 Bryant Harris, Congress reporter for Defense News, formerly wrote for Foreign Policy, Al-Monitor, Al Jazeera English and IPS News, “Document reveals $14 billion backlog of US defense transfers to Taiwan,” Defense News, 4-14-2022, <https://www.defensenews.com/pentagon/2022/04/14/pandemic-delays-spark-14-billion-backlog-of-us-defense-transfers-to-taiwan/> /GoGreen!

Pandemic-related acquisition issues have sparked a backlog in the U.S. delivering $14.2 billion worth of military equipment to Taiwan that the island has purchased since 2019.

With much of Washington’s attention focused on how to rapidly deploy a steady stream of military aid to Ukraine, some lawmakers are concerned the Taiwan delay is undermining its ability to deter a potential Chinese invasion.

Rep. Steve Chabot, the top Republican on the House’s Asia and Pacific panel, told Defense News that the Foreign Affairs Committee held a meeting to discuss the backlog last week.

“We need to make sure that we provide Taiwan with the assistance that they need as well so that they’re not vulnerable to the [People’s Republic of China],” the lawmaker from Ohio said. “Obviously Ukraine is in the limelight right now — and rightfully so — but we best not forget about Taiwan because China’s actions have been more and more provocative.”

Defense News has obtained a spreadsheet detailing the backlogged equipment, which includes Taiwan’s $8 billion purchase of 66 F-16 fighter jets as well as $620 million to replace expiring components of its Patriot missile system.

The delayed deliveries also consist of smaller, asymmetric weapons systems Washington believes would be useful in deterring and thwarting a potential Chinese invasion. China considers the self-governing island a rogue province and has promised to bring it back under Beijing’s control, by force if necessary.

Those asymmetric weapons include Stinger missiles, heavyweight torpedoes, high-mobility artillery rocket systems, Paladin howitzers, MS-110 reconnaissance pods and a field information communications system. They also include $2.37 billion in Harpoon Block II surface-launched missiles and $1 billion in air-launched SLAM-ER missiles.

The $14.2 billion backlog of sales accounts for the vast majority of the approximately $17 billion in military equipment Taiwan agreed to purchase from the United States since July 2019. The U.S. State Department notified Congress of another $95 million sale to provide contracting support for Taiwan’s Patriot missile system just last week. (Foreign Military Sales notification figures represent potential arms sales that the State Department internally clears. They must then clear a congressional review period, during which costs and quantities can change.)

Neither the Defense Department nor Taiwan’s diplomatic office in Washington replied to Defense News’ request for comment about the backlog.

But Taiwan’s envoy to the United States, Hsiao Bi-khim, raised the alarm bells on Capitol Hill last week in a bid to urge Washington to address the backlog.

Hsiao addressed it during a breakfast with Rep. Mike McCaul, R-Texas, the ranking member of the House Foreign Affairs Committee, and pushed for Taiwan’s inclusion alongside the U.S. and more than two dozen other participants in the biennial Rim of the Pacific naval exercises off the coast of Hawaii.

“Her biggest complaint to us is that while we have notified and signed off on these systems, they have yet to be delivered to Taiwan,” McCaul told the State Department’s No. 2 diplomat, Wendy Sherman, during a hearing last week on the Indo-Pacific region.

He likened Taiwan’s position vis-a-vis China to that of Ukraine in the lead-up to the Russian invasion.

“Is Taiwan able to defend herself?” McCaul asked. “I think the answer is ‘no’ right now, and I’m worried about that. I don’t want to make the same mistake of waiting until after an invasion because that’s going to be too late.”

However, it remains unclear what — if anything — the United States can do to address the pandemic-related acquisition issues that prompted the backlog.

“Our primary issue — and we see this playing out in Ukraine also — is that the industry has been delayed in the development of these systems,” a Republican staffer on the House Foreign Affairs Committee told Defense News.

The staffer also noted the U.S. defense industry has attributed supply chain issues, staff shortages and shipping delays to COVID-19 — problems that have cascaded into broader production troubles.

“Honestly, the bottom line is there is very little that the government can do at this juncture to address supply chain issues,” Rupert Hammond-Chambers, the president of the US-Taiwan Business Council, told Defense News.

Hammond-Chambers pointed to the federal government’s inability to address semiconductor supply chain issues that contributed to higher car prices around the globe.

“There’s a great deal of political and international pressure to sort it out, but it’s having almost negligible impact on the ability of the companies to produce the chip that is necessary for the auto industry,” he said.

Prior to the backlog, Congress had largely remained focused on incentivizing Taiwan to make cheaper purchases consisting of large quantities of asymmetric munitions versus the more expensive, state-of-the-art weapons that China may quickly incapacitate during an invasion.

And while much of Taiwan’s U.S. defense purchases bolster its asymmetric capabilities — including many of the backlogged articles — some in Washington raised their eyebrows in 2019 when Taipei opted to move ahead with a $2 billion purchase of Abrams tanks.

“The United States encourages Taiwan to purchase weapons that will enable [it] to adopt a strategy of denial that will prevent China from being able to seize and control Taiwan, so that it will not have the confidence to do so and therefore will not be tempted to do so,” Bonnie Glaser, the Asia Program director at the German Marshall Fund, told Defense News.

For instance, Chabot introduced a bill last year with Rep. Ami Bera, D-Calif., calling on Taiwan to further invest in asymmetric defense capabilities.

Sen. James Risch, R-Idaho, the ranking member on the Senate Foreign Relations Committee, has also introduced a bill to authorize $2 billion a year in Taiwanese military aid, but only if Taipei produces long-term plans for joint capability development with the United States.

Another bill, introduced by Sen. Josh Hawley, R-Mo., would authorize $3 billion in Taiwanese military aid annually. The bill would place more explicit requirements stipulating the funding go toward developing Taipei’s asymmetric defense capabilities against China.

The Biden administration has also encouraged Taiwan to invest more in its asymmetric capabilities, even as many of those munitions remain backlogged.

“We are also encouraging Taiwan to focus on capabilities that would deter the [People’s Republic of China] from taking Taiwan by force,” Sherman said during her testimony before Congress last week. “This means a focus on capabilities that are cost-efficient, mobile, lethal, resilient and capable of operating and surviving a contested environment.”

#### No black swan crisis is coming – empty speculation

Sprenger 22 Sebastian Sprenger, Europe editor and former managing editor for Defense News; Joe Gould, senior Pentagon reporter for Defense News; “US military readies to ‘walk and chew gum’ as multiple crises loom,” Defense News, 1-28-2022, <https://www.defensenews.com/global/europe/2022/01/28/us-military-readies-to-walk-and-chew-gum-as-multiple-crises-loom/> /GoGreen!

Pivot from Asia

Some suggest fears of China invading Taiwan in concert with a Russian invasion of Ukraine are unfounded and have been fueled by overheated rhetoric from both sides.

Retired U.S. Army Lt. Gen. Charles Hooper, who served as director of the Defense Security Cooperation Agency and defense attache in Beijing, said he sees simultaneous invasions of Ukraine and Taiwan as unlikely.

“I assess there’s always a probability of simultaneous crises, and honestly, I believe that the Chinese are watching this current situation very carefully. They will watch to see what [the] Russians do, watch the world react, internalize the lessons learned and then subsequently incorporate that into their own strategy,” Hooper said at a virtual event on Tuesday. “So, in other words, I don’t see things happening simultaneously.”

Even if the U.S. won’t commit troops to defend Ukraine, China should not — and likely will not — see that as a green light for China to invade Taiwan, said Ian Bremmer, president of political risk consultancy Eurasia Group. America has signaled Taiwan is off-limits through its new security pact with Australia and the U.K., the Quadrilateral Security Dialogue, its strengthened diplomacy with Taiwan and this week’s naval exercises with Japan, he argued.

“If anything, the takeaway the Chinese would get from everything over the last year is that America is focused on the areas they care about. Asia is the place they care about and China is the adversary they’re concerned about,” Bremmer said. “We’re both sending signals to each other there here are some fairly significant red lines we both have.”

# AFF AT: DA—DoD O/S

### AT: GPC !

#### “Strategic competition” is meaningless and counterproductive

Nexon 21 Daniel H. Nexon, Professor in the Department of Government and at the Edmund A. Walsh School of Foreign Service at Georgetown University, “Against Great Power Competition,” Foreign Affairs, 2-15-2021, <https://www.foreignaffairs.com/articles/united-states/2021-02-15/against-great-power-competition> /GoGreen!

In his first days in office, U.S. President Joe Biden has worked to signal a clean break with his predecessor. He rejoined the Paris climate accord, offered to extend the New START nuclear weapons treaty, and reversed the “Mexico City” policy curtailing overseas abortion access. His appointees have repeatedly emphasized that the administration will prioritize diplomacy and multilateralism over former President Donald Trump’s “America first” nationalism.

But the fate of a central plank of Trump’s foreign policy remains uncertain: the focus on great-power competition, which according to his administration’s National Security Strategy has “returned.” In a major address at the U.S. State Department, Biden underscored his intention to “work with Beijing when it’s in America’s interests to do so,” but days later noted the likelihood of “extreme competition” with China. This rhetoric may reflect either pragmatism or that great-power competition is on its way to assuming a dominant place in Biden administration policy. Even if Biden aims to de-emphasize competition in certain areas, though, Republicans are certain to criticize the administration for being weak and ineffective in the face of international challenges. Absent some major change in the global threat environment, great-power competition will remain a focal point in debates over U.S. foreign and national security policy.

This is unfortunate. For all the concept’s influence in recent years, great-power competition is not a coherent framework for U.S. foreign policy. Treating it as a guiding principle of American grand strategy risks confusing means and ends, wasting limited resources on illusory threats, and undermining cooperation on immediate security challenges, such as climate change and nuclear nonproliferation. In the long run, a fixation on great-power competition is likely to undermine, rather than enhance, U.S. power and influence.

THE PROBLEM WITH COMPETITION

According to the Trump administration’s 2018 National Defense Strategy, “Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.” Just a year later, the analyst Uri Friedman observed in The Atlantic that great-power competition was now “invoked from Aspen to Israel to South Korea, and by U.S. officials making the case for all sorts of policies.” The phrase, he noted, “has even achieved hallowed acronym status” in the form of “GPC.” Some in Washington see it as a sequel to the original Cold War, with China taking over for the Soviet Union. Others look to more traditional geopolitical rivalries as a model.

Great-power competition’s newfound popularity reflects real facts on the ground. Indeed, competition among great powers cannot return, because it never really went away. Rivalries between leading states exist in every international system. Even during the 1990s—the height of the “unipolar moment”—the United States and Russia competed in the Balkans; the United States and France competed in parts of Africa; and multiple states competed for influence in Central Asia.

But with Washington’s unipolar status now on the wane, powers such as China and Russia find it easier than they once did to challenge U.S. leadership. Since states tend to consider overt antagonism a more attractive option when they expect to come out on top, there will inevitably be more competition among great powers as U.S. relative power declines. With Washington on the back foot, foreign leaders see a chance to gain economically, advance their security interests, and challenge existing norms, rules, or their position in the international pecking order.

It is one thing, though, for Washington to observe increasing competition among great powers and adjust to a world in which it enjoys less influence than it once did. It is another entirely to elevate competition itself to the guiding paradigm of U.S. foreign policy—as the Trump administration proposed and Biden may wind up doing. The mere fact of a more competitive international environment does not compel states to engage in unrelenting struggle. Instead, periods of intense interstate rivalry happen when great powers choose—sometimes as a matter of grand strategy, other times through the accretion of individual tactical decisions—to prioritize conflict over cooperation. Nothing, for instance, requires the United States to push back against every peripheral challenge to its influence, status, or policy preferences. Not every move by Moscow or Beijing constitutes a direct threat to Washington’s national interests.

It is also misguided to think, as some have suggested, that great-power competition makes norms, rules, and other aspects of international order (liberal or otherwise) irrelevant. Even during the Cold War, the United States and the Soviet Union worked out a variety of formal and informal rules that helped them manage competition, limit nuclear proliferation, and otherwise structure international relations. Breaking those rules meant real reputational costs, as the number of covert interventions during the Cold War attests. Both sides of the conflict faced stiff resistance when they violated norms of sovereignty or national self-determination.

These norms, rules, and institutions often complement power politics. They serve as both objects and instruments of great-power contestation. In the nineteenth century, for instance, the German statesman Otto von Bismarck appealed to shared norms in a successful effort to reduce European resistance to German unification. Today, the United States draws much of its relative power from institutional arrangements—notably its unrivaled network of alliances and partnerships—that frequently reflect and derive legitimacy from liberal values.

These relationships underscore a central problem with treating great-power competition as the organizing principle of foreign policy: it provides very little in the way of guidance to policymakers. There is no single grand strategy for eras of great-power competition. There are no instruments of statecraft that competition renders relevant or irrelevant. Great-power competition doesn’t even imply adopting a more antagonistic approach to rivals: as U.S. President Ronald Reagan and Soviet leader Mikhail Gorbachev realized by 1987, the best response to intensifying competition may be to dial tensions back through confidence-building measures and cooperation.

Such indeterminacy helps explain the concept’s widespread appeal: one can use great-power competition to justify almost anything. In the 1990s, the United States needed enormous military budgets to prevent the emergence of new great-power competitors. Now it needs them to compete with existing ones. Liberals once called for major investments in infrastructure, education, and research to sustain American primacy. Now they call for them to keep the United States competitive in a multipolar world. Great-power competition might require strategic retrenchment, or offshore balancing, or deep engagement. Perhaps it means that Washington must give up its liberal illusions and pursue unbridled and unilateral realpolitik. Or maybe the United States needs to commit to multilateralism and more equitable relationships with allies.

#### Their impact theorizations overstate the scope of competition – it’s NOT all-encompassing, revisionism is selective – our advantages have greater explanatory power – theirs backfire

Ashford 21 Emma Ashford, senior fellow at the Atlantic Council’s Scowcroft Center for Strategy and Security, “Great-Power Competition Is a Recipe for Disaster,” Foreign Policy, 4-1-2021, <https://foreignpolicy.com/2021/04/01/china-usa-great-power-competition-recipe-for-disaster/> /GoGreen!

“America is back,” blared headlines following President Joe Biden’s speech to the Munich Security Conference in February, an address clearly designed to draw a line under the Donald Trump presidency and mark a new start in trans-Atlantic relations. “We are not looking backward,” Biden promised. “We are looking forward, together.” Yet one big plank of the Trump administration’s foreign policy is apparently sticking around: great-power competition. “We must prepare together for a long-term strategic competition,” Biden told conference attendees, adding that “competition with China is going to be stiff.”

Unfortunately, for all that great-power competition has been Washington’s favorite buzzword in recent years, it remains frustratingly poorly defined. Indeed, most commentators skip right past the big questions (Why are we competing? Competing over what?) and go straight to arguing about how to achieve victory. Since the possible answers to these questions range from the entirely reasonable (i.e., that Western states should engage in collective defense of liberal democracy) to the dangerous and utterly unrealistic (i.e., that Washington should be pursuing regime collapse in Beijing), it’s hardly something we should ignore.

It seems that once again—just as it did during the global war on terrorism in the mid-2000s or when styling the United States as the indispensable nation in the 1990s—Washington’s strategic community is again reorienting itself around a new, poorly theorized model of the world and of America’s place in it. Yet precisely because it is so ill-defined, great-power competition as a strategy—that is to say, competition for its own sake—also has the potential to be highly dangerous.

It is a mark of how recently the notion of great-power competition has entered the Washington lexicon that someone who had fallen into a coma just five years ago might never have heard the phrase. Though the Obama administration’s 2015 National Military Strategy warned of states “attempting to revise key aspects of the international order,” it was not until the Trump era that the term itself entered widespread use. Then-U.S. Defense Secretary James Mattis said in June 2017 that a “return to great-power competition … places the international order under assault,” while the National Security Strategy released later that year noted that “after being dismissed as a phenomenon of an earlier century, great power competition returned.” Since then, its growth has been exponential.

As a description, great-power competition is accurate; competition among the great powers is a defining feature of the international environment. Whether one is talking about 16th-century rivalries among empires, the imperialist scramble for Africa, or the Cold War struggle between the capitalist and communist blocs, states have always jockeyed for power and influence. But the notion that it is new—or that it is returning as if history were taking its revenge—is somewhat absurd. As the Georgetown University professor Daniel Nexon recently put it, “competition among great powers cannot return, because it never really went away.”

Instead, the “return of great-power competition” is essentially an easier way of admitting that the United States is in relative decline. The unipolar moment—the three-decade period of U.S. global predominance that started with the collapse of the Soviet Union—is ending. In the parlance of political science, other states are beginning to balance against the United States. In layman’s terms, this means that with the United States in relative decline, other states are increasingly willing to take actions they would not have during the 1990s, whether it’s Russian intervention in Syria, Chinese claims to the South China Sea, or European steps to circumvent U.S. sanctions legislation. Irving Kristol, considered the godfather of neoconservatism, once noted that a neoconservative is just a liberal who’s been mugged by reality; some of the loudest voices proclaiming an era of great-power competition are just liberal internationalists who have been mugged by the reality of power politics.

Yet if this were all there was to it, the debate surrounding great-power competition would be far less problematic. Scholars and pundits would update their mental models for a more competitive world and move on with their lives. Instead, foreign-policy circles in Washington are increasingly fixated on the notion that the United States must commit to competition with China, Russia, and other states.

Great-power competition is portrayed less as a fact of life and more as a strategy in and of itself. Certainly, some authors do suggest a potential endpoint to great-power competition, such as Hal Brands and Zack Cooper, whose recent piece in Foreign Policy argued that competition between the United States and China would only lessen when the regime in Beijing collapsed. But they are still unclear on why we should pursue an existential Cold War-style struggle with China, rather than a more measured approach of competitive coexistence.

This example is emblematic of the debate on great-power competition as a whole. As a grand strategy—what the Yale University professor John Lewis Gaddis once described as “the calculated relationship of means to large ends”—great-power competition is sorely lacking. For starters, it’s not clear whether competition is itself a means or an end.

The 2017 National Security Strategy, for example, describes the world as an “arena of continuous competition” for which the United States must prepare. Whether it is domestic infrastructure projects, student loan forgiveness, repairs to democratic institutions, or increasing the birth rate, a wide range of policy priorities are now portrayed as essential to the pursuit of great-power competition. This suggests that great-power competition is itself an end. Why the country is compelled to compete in this way typically goes unstated.

Indeed, if great-power competition is instead a means to an end, it’s not at all clear what those ends are. There’s rarely a concrete goal among those who proselytize in favor of a strategy of great-power competition. Consider how the topic is portrayed by former National Security Advisor H.R. McMaster in his recent book. He opens by noting that “after the end of the Cold War, America and other free and open societies forgot that they had to compete to keep their freedom, security, and prosperity” while later arguing that states must “compete thoroughly as the best means of avoiding confrontation.” Confusingly, he portrays competition as both an alternative to conflict and as a Manichean struggle between good and evil, with the United States beset by adversaries on all sides.

It’s easy to dismiss this kind of rhetoric as silly, but it also carries substantial danger. For one thing, the focus on competition masks a whole series of underlying assumptions about the international system and America’s role in it. Washington’s policy community appears convinced that we are headed for a more dangerous world, one in which the United States must push back against the perceived aggression of states like China and Russia. Though articles almost always include an obligatory aside—that cooperation with China on climate change is a must!—the frame is almost uniformly confrontational.

To be clear, there are good reasons for Washington’s strategic community to perceive an increasingly competitive world. The gap between the United States and other countries is narrowing militarily; it has already closed by some economic measures. And pushback against U.S. foreign-policy choices among other states has increased in recent years, from Chinese attempts to revise maritime rules to Russia’s aggressive targeting of foreign elections. But a more competitive world isn’t the same thing as an all-out struggle. Great-power competition is often portrayed as an all-or-nothing conflict, where revisionist autocracies are challenging the United States in every sphere. In reality, thus far China and Russia are only selectively revisionist, attempting to change the status quo where it suits their interests and to maintain it in other places.

The risks of the all-or-nothing approach to global politics cannot be overstated. As Fareed Zakaria put it recently, “The United States risks squandering the hard-won gains from four decades of engagement with China, encouraging Beijing to adopt confrontational policies of its own, and leading the world’s two largest economies into a treacherous conflict of unknown scale and scope.” Indeed, if one assumes—as much of the writing on great-power competition does—that China and Russia are implacable foes of the United States determined to destroy the existing order and overturn U.S. hegemony, then policies that would otherwise be unthinkable are suddenly on the table.

Military buildup in Europe and Asia becomes necessary, even if it raises the risk of open conflict with another nuclear power. Economic decoupling seems vital to protect supply chains, though studies show that the costs to U.S. companies and workers would be extreme. A recent report by the U.S. Chamber of Commerce’s China Center, for example, estimated that the U.S. economy could lose up to $1 trillion in growth if tariffs were more broadly applied to all U.S.-China trade. Restrictions on tourism or on Chinese students studying in the United States would cost between $15 billion and $30 billion per year.

The bottom line is simple: It’s easy to make fun of great-power competition as a meaningless buzzword or as Washington’s foreign-policy elite rediscovering that other states get to have a say in world politics. But as the political scientist Robert Kagan wrote recently, the biggest question of the coming decades may be whether countries can “confine the global competition to the economic and political realms and thus spare themselves and the world from the horrors of the next great war or even the still frightening confrontations of another cold war.” In that context, the blind pursuit of a strategy of great-power competition is irresponsible and shortsighted.

The last time the United States single-mindedly pursued a poorly thought-out slogan masquerading as a strategy, it ended up fighting a two-decade global war on terrorism, a conflict from which it is still struggling to extricate itself and that had immense negative effects on the country’s foreign relations and its domestic liberties. Yet if today’s leaders are not careful, the rhetoric of great-power competition could drag the United States into a conflict even more costly and damaging.

#### No impact to losing – and “rules-based order” is NOT at stake

Fettweis 20 – Dr. Christopher Fettweis, Professor at Tulane University’s Department of Political Science, President of the board of the World Affairs Council of New Orleans, PhD from the University of Maryland, adjunct scholar in the Cato Institute’s Defense and Foreign Policy Studies Department; “Delusions of Danger: Geopolitical Fear and Indispensability in U.S. Foreign Policy;” 06-03-20, Cato Institute, <https://www.cato.org/publications/delusions-danger-geopolitical-fear-indispensability-us-foreign-policy>; Go Green! \*added [obfuscate]

The Indispensable Nation

Although geopolitical fear prevents current international empirical realities from receiving a fair evaluation by U.S. society, another belief prescribes a specific approach to foreign policy, one that mandates a far higher level of international activism than would otherwise be warranted. Both are based on thin intellectual foundations, and together they encourage a variety of ill‐​advised policies on the part of the United States. According to what might be considered the indispensability fallacy, many Americans believe that U.S. actions are primarily responsible for any stability that currently exists. “All that stands between civility and genocide, order and mayhem,” explain Lawrence Kaplan and William Kristol, “is American power.“37 That belief is an offshoot, witting or not, of what is known as “hegemonic stability theory,” which proposes that international peace is possible only when one country is strong enough to make and enforce a set of rules.38 Were U.S. leaders to abdicate their responsibilities, that reasoning goes, unchecked conflicts would at the very least bring humanitarian disaster and would quite quickly threaten core U.S. interests.39

Brzezinski is typical in his belief that “outright chaos” and a string of specific horrors could be expected to follow a loss of hegemony, from renewed attempts to build regional empires (by China, Turkey, Russia, and Brazil) to the collapse of the U.S. relationship with Mexico as emboldened nationalists south of the border reassert 150‐​year‐​old territorial claims. Overall, without U.S. dominance, today’s relatively peaceful world would turn “violent and bloodthirsty.“40 The liberal world order that is so beneficial to all would come tumbling down.

Like many believers, proponents of hegemonic stability theory base their view on faith alone.41 There is precious little evidence to suggest that the United States is responsible for the pacific trends that have swept across the system. In fact, the world remained equally peaceful, relatively speaking, while the United States cut its forces throughout the 1990s, as well as while it doubled its military spending in the first decade of the new century.42 Complex statistical methods should not be needed to demonstrate that levels of U.S. military spending have been essentially unrelated to global stability.

Hegemonic stability theory’s flaws go way beyond the absence of simple correlations to support them, however. The theory’s supporters have never been able to explain adequately how precisely 5 percent of the world’s population could force peace on the other 95 percent, unless, of course, the rest of the world was simply not intent on fighting. Most states are quite free to go to war without U.S. involvement but choose not to. The United States can be counted on, especially after Iraq, to steer well clear of most civil wars and ethnic conflicts. It took years, hundreds of thousands of casualties, and the use of chemical weapons to spur even limited interest in the events in Syria, for example; surely internal violence in, say, most of Africa would be unlikely to attract serious attention of the world’s policeman, much less intervention. The continent is, nevertheless, more peaceful today than at any other time in its history, something for which U.S. hegemony cannot take credit.43 Stability exists today in many such places to which U.S. hegemony simply does not extend.

Overall, proponents of the stabilizing power of U.S. hegemony should keep in mind one of the most basic observations from cognitive psychology: rarely are our actions as important to others’ calculations as we perceive them to be.44 The so‐​called egocentric bias, which is essentially ubiquitous in human interaction, suggests that although it may be natural for U.S. policymakers to interpret their role as crucial in the maintenance of world peace, they are almost certainly overestimating their own importance. Washington is probably not as central to the myriad decisions in foreign capitals that help maintain international stability as it thinks it is.

The indispensability fallacy owes its existence to a couple of factors. First, although all people like to bask in the reflected glory of their country’s (or culture’s) unique, nonpareil stature, Americans have long been exceptional in their exceptionalism.45 The short history of the United States, which can easily be read as an almost uninterrupted and certainly unlikely story of success, has led to a (perhaps natural) belief that it is morally, culturally, and politically superior to other, lesser countries. It is no coincidence that the exceptional state would be called on by fate to maintain peace and justice in the world.

Americans have always combined that feeling of divine providence with a sense of mission to spread their ideals around the world and battle evil wherever it lurks. It is that sense of destiny, of being the object of history’s call, that most obviously separates the United States from other countries. Only an American president would claim that by entering World War I, “America had the infinite privilege of fulfilling her destiny and saving the world.“46

Although many states are motivated by humanitarian causes, no other seems to consider promoting its values to be a national duty in quite the same way that Americans do. “I believe that God wants everybody to be free,” said George W. Bush in 2004. “That’s what I believe. And that’s one part of my foreign policy.“47 When Madeleine Albright called the United States the “indispensable nation,” she was reflecting a traditional, deeply held belief of the American people.48 Exceptional nations, like exceptional people, have an obligation to assist the merely average.

Many of the factors that contribute to geopolitical fear — Manichaeism, religiosity, various vested interests, and neoconservatism — also help explain American exceptionalism and the indispensability fallacy. And unipolarity makes hegemonic delusions possible. With the great power of the United States comes a sense of great responsibility: to serve and protect humanity, to drive history in positive directions. More than any other single factor, the people of the United States tend to believe that they are indispensable because they are powerful, and power tends to [obfuscate] ~~blind~~ states to their limitations. “Wealth shapes our international behavior and our image,” observed Derek Leebaert. “It brings with it the freedom to make wide‐​ranging choices well beyond common sense.“49 It is quite likely that the world does not need the United States to enforce peace. In fact, if virtually any of the overlapping and mutually reinforcing explanations for the current stability are correct, the trends in international security may well prove difficult to reverse. None of the contributing factors that are commonly suggested (economic development, complex interdependence, nuclear weapons, international institutions, democracy, shifting global norms on war) seem poised to disappear any time soon.50 The world will probably continue its peaceful ways for the near future, at the very least, no matter what the United States chooses to do or not do. As Robert Jervis concluded while pondering the likely effects of U.S. restraint on decisions made in foreign capitals, “It is very unlikely that pulling off the American security blanket would lead to thoughts of war.“51 The United States will remain fundamentally safe no matter what it does — in other words, despite widespread beliefs in its inherent indispensability to the contrary.

### AT: Alliances !

#### No war from abandonment nor entanglement

Fisher 16 Max Fisher, foreign editor at Vox, former reporter and founding editor of the WorldViews foreign affair blog at The Washington Post, MA International Relations and Affairs, Johns Hopkins University School of Advanced International Studies, “The Credibility Trap,” Vox, 4-29-2016, <https://www.vox.com/2016/4/29/11431808/credibility-foreign-policy-war> /GoGreen!

If reputational credibility has been so repeatedly debunked, both in specific instances and as a theory, why does it continue to loom so large in America's foreign policy discourse?

Tufts University's Michael Beckley hinted at one possible explanation in a much-discussed article last year in International Security: Could it have something to do with America's uniquely broad network of alliances?

Beckley's article was actually asking a different question — whether those alliances lead the US to war, by allowing allies to "entangle" it in foreign conflict. (Beckley concludes the answer is no; other scholars have disputed his findings.)

But, in reviewing so-called "entanglement theory," Beckley points out that reputational credibility, even if it doesn't exist in the world, is something that definitely exists in the minds of foreign leaders and foreign policy decision-makers.

"The alliance comes to be perceived as an end in itself, transcending the more concrete national security interests for which it was initially conceived," political scientist Jack Levy wrote in a well-known 1981 paper (which Beckley cites). Here's the key quote:

Political decision makers come to believe that support for one's allies, regardless of its consequences, is essential for their national prestige, and that the failure to provide support would ultimately result in their diplomatic isolation in a hostile and threatening world.

So it's not that reputation is a real thing that compels states to act in a certain way, but rather that individual decision-makers are driven by their own mistaken belief in reputation. As a result, Beckley writes, "reputational concerns can drive states into wars over trivial interests in peripheral places."

Some scholars, including Levy, argue that America's allies promote the idea of reputation, as a means to convince the United States to commit more resources to serve their own interests.

Foreign leaders do seem to become awfully preoccupied with American credibility when they want the US to take military action on their behalf. When the US failed to bomb Syria in 2013, for example, Syria's enemies in the region — Arab leaders who are also allied with the US — declared that American credibility was at stake.

"I think I believe in American power more than Obama does," Jordan's King Abdullah II said of Obama's decision to not bomb Syria.

This comes at a time when the US has grown unusually indulgent of its allies, as Jeremy Shapiro and Richard Sokolsky argue in a recent article. This has made American policymakers more likely to heed allies' demands and take their claims at face value.

But Dartmouth's Jennifer Lind finds evidence that allies make this argument only opportunistically, and almost always about conflicts in which they are directly involved. They might speak in the language of reputation theory, but their behavior suggests that they do not really believe in it.

Reputation theory, after all, says that America's allies would want the US to intervene as much as possible in other conflicts, when in fact the opposite is usually true.

### AT: Demo I/L

#### SC can’t solve democracy

Miller 21 Aaron David Miller, Global Fellow at the Woodrow Wilson International Center for Scholars, former Senior Advisor for Arab-Israeli Negotiations at the State Department, PhD American Diplomatic and Middle East History, University of Michigan; and Richard Sokolsky, nonresident senior fellow in Carnegie’s Russia and Eurasia Program, former director of the offices of Strategic Policy and Negotiations, Policy Analysis, and Defense Relations and Security Assistance in the State Department’s Bureau of Political-Military Affairs, MA Johns Hopkins University School of Advanced International Studies; “Biden is right that global democracy is at risk. But the threat isn’t China,” The Washington Post, 12-3-2021, <https://www.washingtonpost.com/outlook/democracy-summit-china-russia/2021/12/03/d64d4544-537a-11ec-8769-2f4ecdf7a2ad_story.html> /GoGreen!

There are many good reasons to host such a gathering. It’s smart politics, fulfills a campaign commitment and counters the perception, fostered by President Donald Trump, that America is no longer interested in promoting democracy and human rights. But as a geopolitical instrument, drawing lines between democracies and autocracies is not only certain to disappoint — it’s also a deeply flawed organizing principle for America’s approach to the world.

China and Russia, which Biden has also singled out for criticism, are not the main causes of the weakening of democracies around the world. Most of the backsliding, according to a recent study, has been caused by erosion within the world’s democracies, including the United States and many of its allies. Indeed, the upcoming summit includes a number of countries — India, Brazil, the Philippines and Poland among them — marked by growing autocratic movements and infringements on freedom of expression and a free press. And pushing these and other countries to reform their political, electoral or judicial institutions from the outside is hard if not impossible.

Biden isn’t the first and won’t be the last American president to make democracy promotion central to his foreign policy. Woodrow Wilson wanted to make the world “safe for democracy”; Franklin Roosevelt promulgated the Atlantic Charter. The Clinton administration was present at the creation of the Community of Democracies. George W. Bush had his Freedom Agenda and talked about ridding the world of dictators. All found democracy promotion a useful tool to advance U.S. values and interests.

Biden seems to genuinely believe that democrats and dictators are in a do-or-die battle over who will own the 21st century. Though he insists that he doesn’t want a new cold war, some of his overcharged rhetoric belies this view. In March, Biden announced his intention “to invite an alliance of democracies to come here to discuss the future,” including holding “China accountable to follow the rules” on issues such as persecution of its Uyghur citizens and its territorial disputes with Taiwan. Biden has said of China’s President Xi Jinping that he “doesn’t have a democratic bone . . . in his body” and that Xi believes “democracy cannot keep up with” China.

It is simplistic to believe, however, that Chinese and Russian foreign policies are driven by the ideological impulse to spread autocracy. Both countries see the United States as their main geopolitical adversary and seek to undermine American influence and alliances wherever they can; the Chinese are also bent on outcompeting the United States in 21st-century technologies.

But the Russians don’t have an authoritarian model for export, and other autocratic-minded governments don’t need inspiration from Moscow to run kleptocratic, corrupt, repressive and misgoverned regimes. Putin’s overriding priority is self-preservation and the preservation of his regime. What evidence is there that he believes these objectives can be achieved only if the rest of the world looks like Russia?

Likewise, Xi’s main priority is maintaining his control and the Chinese Communist Party’s monopoly on power. He is all too happy to claim that the Chinese government is outperforming America’s dysfunctional system. But it is simply not the case that he thinks these goals require Beijing to actively spread authoritarianism with Chinese characteristics abroad. And China’s wealth and power, not to mention its social stability, depend on competing effectively within the interdependent global economic system, not toppling it.

Another flaw in the Biden administration’s approach is the presumption that all democracies think alike based on their shared commitment to democratic values. If only it were that simple. Values do shape a nation’s foreign policy, but history, geography, culture, political ideology and material interests also matter. It is precisely for these reasons that America’s democratic allies and partners do not see eye to eye on how to deal with China or Russia — and why they shouldn’t be forced to choose sides between the United States and the authoritarians.

#### US backsliding thumps

Miller 21 Aaron David Miller, Global Fellow at the Woodrow Wilson International Center for Scholars, former Senior Advisor for Arab-Israeli Negotiations at the State Department, PhD American Diplomatic and Middle East History, University of Michigan; and Richard Sokolsky, nonresident senior fellow in Carnegie’s Russia and Eurasia Program, former director of the offices of Strategic Policy and Negotiations, Policy Analysis, and Defense Relations and Security Assistance in the State Department’s Bureau of Political-Military Affairs, MA Johns Hopkins University School of Advanced International Studies; “Biden is right that global democracy is at risk. But the threat isn’t China,” The Washington Post, 12-3-2021, <https://www.washingtonpost.com/outlook/democracy-summit-china-russia/2021/12/03/d64d4544-537a-11ec-8769-2f4ecdf7a2ad_story.html> /GoGreen!

There’s also the politically inconvenient question of whether the United States is best positioned to lead this effort. Rarely has America’s democracy crusade abroad contrasted more with its commitment to democratic practices at home — where the threats include Trump’s false claims that the presidential election was “stolen,” an insurrection to stop a democratic transition and efforts to restrict voting rights. America has a glass-house problem, and it needs to promote its democratic virtues with considerable humility. According to Freedom House’s annual country-by-country assessment of political and civil rights, the United States continued to experience erosion in democratic practices in 2020;over the past decade, America’s score dropped from 94 to 83 out of 100, among the steepest falls of any country during this period.

It is hard to take seriously the notion that the United States can restore its “soft power” by virtue of the example it is setting at home. A recent Pew Research Center study found that a median of only 17 percent of people in surveyed countries thought U.S. democracy worth emulating, while 23 percent said it had never offered a good example. It is also hard to quibble with the proposition that America’s influence abroad is waning primarily because of its domestic problems, rather than authoritarian muscle-flexing in Moscow or Beijing.

### AT: Demo ! – DPT

#### No impact to democracy – confounding variables control

Doorenspleet ’19 [Renske; 2019; Political Science and International Studies Professor at Warwick University; Rethinking the Value of Democracy: A Comparative Perspective, “Democracy and Interstate War,” Ch. 3]

This finding or ‘law’ has not only been recognized by scholars of international relations, but also found its way outside academia and has influenced foreign policies to promote peace and democracy, most prominently since the 1990s. However, my book will not draw conclusions based on ‘cherry-picking’ of specific studies showing how peaceful democracies are, but on a systematic overview of studies in this field. Therefore, this book relies on my own database with hundreds of different studies, which are relevant for each chapter; the articles had to engage directly with the chapter’s main research question. The next section will provide more detailed information around the selection criteria. This overview includes both highly cited and recent articles which were selected in a systematic way.

Based on analyses of statistical studies around this topic of democracy and war, it will become clear that the overall statistical support for the democratic peace hypothesis is not strong at all. In the rest of the chapter, I will spell out four reasons why democracy does not cause peace, and why the empirical support for the popular idea of democratic peace is quite weak: (1) most studies do not find a strong correlation between democracy and interstate war at the dyadic level, and they show that there are other—more powerful—explanations for war and peace, or even that the impact of democracy is a spurious one, (2) the theoretical foundation of the democratic peace hypothesis is weak, and the causal mechanisms are unclear, (3) democracies are not necessarily more peaceful in general, and the evidence for the democratic peace hypothesis at the monadic level is inconclusive, and (4) the process of democratization is dangerous and living in a democratizing country means living in a less peaceful country.

In my view, it is difficult—if not impossible—to support the democratic peace hypothesis without any reservations. The key caveats should not be ignored and certainly deserve more attention before we can confidently argue that democracies are more peaceful than other types of political systems. Please notice that I can already reveal that the assumed link between democracy and intrastate war is problematic as well, but this topic will be at the core of the next chapter (Chapter 4).

Selection of Articles: Democracy and War

The instrumental value of democracy cannot convincingly be found in democracy’s expected bond with peace. I have come to this conclusion on the basis of an analysis of statistical studies, which will be discussed in the rest of this chapter. So how did I select the articles for my database?4

For this chapter and Chapter 4, I selected the articles that focused on war and democracy. Using the online database Web of Science (formerly known as Web of Knowledge), I identified a total of almost 8000 articles published in the sampled journals until the end of 2015. I identifed them by entering ‘democr\*’ in the basic search field; this asterisk (\*)-based ‘wildcard’ allows searching for terms including ‘democratic’, ‘democracy’, and ‘democratization’ (in both British and American spellings) simultaneously, in the title, abstract and/or the keywords. As a next step, I excluded articles in which ‘democracy’ is used as synonym for state (e.g. analysis of the relationship between immigration policies and unemployment in European democracies) or a specific political party or movement (e.g. the ‘Democrats’ in the USA, or Uganda’s People’s Democratic Army) or a specifc country (e.g. the Democratic Republic of Congo). In addition, I identified them by entering ‘war\*’ in the basic search feld. The words democracy (democr\*) and war (war\*) need to be mentioned in title and/or abstract—and I also checked for equivalents of ‘war’ like ‘conflict’ and ‘dispute’ and ‘no peace’.5

As it is not feasible to analyse thousands of articles, it is necessary to take a next step in the selection process. I decided to select these articles, which will be part of the database for the third and fourth chapter, in three different ways. The first method is to choose the articles with the most citations. So, for example, in Chapter 3, the articles which are cited more than a hundred times are included in this first list. The article by Beck et al. (1998) has been cited more than 951 times, and as a consequence, this article is part of the database. But also articles with a much lower number of citations (such as Barbieri 1996, with 179 citations) are included in my analyses.

The second method is simply to include the most recent articles published in the past five years, so since beginning 2011 until end 2015. The most recent articles can easily be overlooked by applying the first method of most quoted articles. In my view, however, they still need to be included as they present the most recent findings and engage with the recent and innovative debates, which cannot be ignored in this book. For example, recent studies on democracy and interstate war (Chapter 3) have paid more attention to the mechanisms (see, e.g., Zeigler et al. 2014), and there is a growing attention for the impact of political institutions in recent studies on democracy and intrastate war (Chapter 4; see, e.g., Walter 2015). Those recent findings cannot be ignored in any systematic analysis of statistical studies on this theme.

The third method is the most subjective approach of selecting articles, as it is based on the ‘snowballing method’. So it includes articles which have not been selected by the first and second methods, but which have been quoted extensively and regularly by the previously selected articles. For example, the article by Bethany Lacina (2006) cannot be selected based on having high citations (the first method) and it cannot be included based on being a recent publication (the second method), but it has been mentioned by key studies and hence surfaces via the snowballing method (a third method). This article is important as it clearly distinguishes the determinants of conflict severity from those for conflict onset, and those determinants seem to be quite different, which is crucial information for Chapter 4.

In this way, my study presents and assesses the findings based on a big pool of statistical studies in the published literature. Based on this assessment, I will be able to draw clearer conclusions concerning the significance of the effects of democracy on interstate war (this chapter) and intrastate war (the next chapter). The Appendix shows more detailed information of the selected articles.

The Democratic Peace Hypothesis, Its Roots and Supporters

The democratic peace hypothesis6 states that democracies never or seldom go to war with one another. Where is this powerful idea of ‘democratic peace’ coming from? Before discussing the main findings of the statistical articles and before describing the four caveats of the ‘democratic peace paradigm’, we need to know a bit more around the background and the roots of this idea.

Immanuel Kant’s 1795 essay Perpetual Peace has often been mentioned as the foundation for this hypothesis. Kant believed peace was difficult to achieve, since ‘the natural state is one of war’ (Kant 1795: 10). A state of peace must therefore be established for—in his view—it is certain that hostilities will be committed and people need to be protected from each other. In such a world, each may treat his neighbour, from whom he demands security, as an enemy. In a dictatorship where ‘the subjects are not citizens, a declaration of war is the easiest thing in the world to decide upon, because war does not require of the ruler, who is the proprietor and not a member of the state, the least sacrifice of the pleasures of his table, the chase, his country houses, his court functions, and the like. He may, therefore, resolve on war as on a pleasure party for the most trivial reasons, and with perfect indifference leave the justification which decency requires to the diplomatic corps who are ever ready to provide it’ (Kant 1795: 13).

In contrast, the situation is different in constitutional republics, according to Kant. He argued that the majority of the people in republics would never vote to go to war, except for pure self-defence. Therefore, a world with only republics would be peaceful, since there would be no aggressors. The republican constitution, which requires the consent of the citizens to start a war, gives the positive prospect of perpetual peace.

It is important to note that the ideas of Kant on the one hand and the modern democratic peace scholars on the other hand are not completely similar. For example, Kant talked about republics instead of democratic states as the ideal states to achieve peace. He defined republican states as states with representative governments, in which the legislature is separated from the executive. Not surprisingly—considering the epoch in which he lived—Kant did not include universal suffrage in his definition, which is now seen as an essential dimension of democracy, even of the most minimalist types of democracy (Dahl 1971; see also Chapter 2). Moreover, Kant argued that republics will be at peace in general, which means that such political systems are expected to be not only in peace with each other, but also with other non-republican systems. Nowadays, only few scholars would support this approach of a ‘monadic democratic peace’. As will become clear at the end of this chapter, there is not much evidence for the idea that democracies are more peaceful in general.

Since the 1960s, most statistical studies have not focused on the ‘monadic democratic peace hypothesis’ but on testing the ‘dyadic democratic peace hypothesis’. This dyadic hypothesis states that it is less likely that democracies fight with each other, compared to other ‘dyads’ or other pairs of different types of political systems. The sociologist Dean Babst was the first scholar who started to build on Kant’s old idea in the ‘dyadic’ way, and decided to test it in statistical studies (Babst 1964, 1972). He concluded that ‘no wars have been fought between independent nations with elective governments between 1789 and 1941’ (Babst 1972: 55). His study was not published in one of the journals in the field of international relations, but in a sociological journal and later in Industrial Research. Therefore, it was not read by international relations scholars, and initially, it did not get the attention it deserved in the field of international politics.

Babst’s work was, for example, not cited by Melvin Small and J. David Singer (1976), and their fndings seemed to contradict Babst’s study. However, Small and Singer did not compare the rates of war proneness for democracies and dictatorships, but instead they focused on the question whether wars involving democratic states have historically been significantly different in length or in degree of violence compared to wars involving only dictatorships. For length and degree of violence during the wars, they did not find a difference between democracies and dictatorships, so they concluded that types of political systems did not matter.7 A few years later, Rudolph J. Rummel did cite Babst’s work and replicated Babst’s idea in statistical tests, which were described in the fourth book of his five-volume Understanding Confict and War (1975– 1981). He found clear support for his eleventh (of the 33) propositions about causes and conditions of conflict, which stated that ‘Libertarian systems mutually preclude violence’ (Rummel 1979: 279).

Eventually, those innovative studies from the 1970s helped to evoke the interest in the democratic peace proposition, and in the expected peaceful nature of relationships among democratic states. Since the 1980s, the number of quantitative studies has increased considerably, accumulating into an impressive field of research in international relations with its own ‘empirical law’ of democratic peace (Levy 1989: 270; see also Ray 1998).

This democratic peace hypothesis has not only received support from political scientists, but also from politicians and policy makers. Particularly since 1993, the idea of a democratic peace has inspired American foreign policies aimed at the promotion of peace and democracy. As the 42nd president of the USA (1993–2001), Bill Clinton was the first politician who explicitly bridged the gap between these findings in international relations on the one hand, and his foreign policy strategy on the other hand, at least rhetorically. Anthony Lake, who was Clinton’s National Security Adviser, stated in 1993 that in order to cope with America’s foreign policy challenges, the expansion of democratic states around the world would be essential because ‘it protects our [U.S.] interests and security’ (see Henderson 2002: 20). In his 1994 State of the Union, Clinton declared that ‘Ultimately, the best strategy to ensure our security and to build a durable peace is to support the advance of democracy elsewhere. Democracies don’t attack each other’.8 Findings from research in the field of international relations seemed to have a direct impact on policy making, and this move of the Clinton administration can be seen as ‘a textbook case of arbitrage between the ivory tower and the real world’ (Gowa 1999: 109).

Clinton’s successor, George W. Bush, went one big step further in his faith that democratic peace holds. He argued that efforts to turn Iraq into a democratic country would have positive effects on Iraqi’s neighbours. The authoritarian regimes in the region would fall as domino stones and follow the Iraqi example. They would start democratizing as soon as they could, which would then result in achieving a peaceful and stable the Middle East. The real motives for attacking Iraq may have been different, but ‘regime change’ was at the heart of Washington’s rhetoric when the USA started to bomb Baghdad in March 2003. The rhetoric of the Bush administration focused on toppling Saddam Hussein’s regime, and replacing the entire underlying dictatorial system with a democracy.

Moreover, George W. Bush used the democratic peace idea to justify the war in Iraq, declaring, ‘The reason why I’m so strong on democracy is democracies don’t go to war with each other…I’ve got great faith in democracies to promote peace. And that’s why I’m such a strong believer that the way forward in the Middle East, the broader Middle East, is to promote democracy’.9 In 2004, the 43rd President of the USA said: ‘If you think you can have peace without democracy – again - I think you’ll find that - I can only speak for myself, that I will be extremely doubtful that it will ever happen’.10 In his second inaugural address, he stated that ‘the survival of liberty in our land increasingly depends on the success of liberty in other lands. The best hope for peace in our world is the expansion of freedom in all the world’.

Again, these are just words from speeches and can hence be seen as rhetoric to defend military intervention (cf. Jervis 2003; Kaufmann 2004; Daalder and Lindsay 2005; Owen 2005; Lieberfeld 2005; Schmidt and Williams 2008). Still, in the end, politicians have rationalized their political decisions based on one of the most powerful ideas taken from studies in the field of international relations, clearly showing the influence of this academic idea in political practice.

Hence, the field of international relations seems to have its own law: democracies rarely fight with each other. It cannot be denied that the evidence supporting the democratic peace proposition is quite diverse in character (see Ray 1998): the evidence has been epistemological (Rummel 1975), philosophical (Doyle 1986), formal (Bueno de Mesquita and Lalman 1992), historical (Weart 1994; Ray 1995; Owen 1994), experimental (Mintz and Geva 1993), anthropological (Ember et al. 1992; Crawford 1994), psychological (Kegley and Hermann 1995), economic (Brawley 1993; Weede 1996) and political (Gaubatz 1991). Still, there have been numerous critical studies (see, i.e., Hayes 2011), and the general picture is unclear. We do not yet know much about the overall findings from statistical studies.

So far, it seems as if some quantitative studies—mainly within the field of international relations—have found strong and robust evidence which supports the ‘democratic peace hypothesis’. Those studies show that democracy has had a positive influence on international peace (see, i.e., Rummel 1979; Ray and Russett 1996). In this sense, the idea of a democratic peace seems to be confirmed. Political scientists such as James Lee Ray are passionate supporters: ‘No scientific evidence is entirely definitive’ but ‘based on all the empirical evidence so far’ the more defensible of the two possible definitive answers to the question “Does democracy cause peace?” is “Yes” (Ray 1998: 43). However, based on my own analyses of the empirical studies with statistical evidence, I cannot be as enthusiastic as those scholars; to the contrary, I whole-heartily disagree with them, as a more systematic analysis of the articles shows that there are four important weaknesses, which seriously undermines the idea that peace is one of democracy’s instrumental values.

Caveat 1: It’s Not (Just) Democracy

While analysing the selected articles, the first remarkable finding is that only a relatively small number of studies have actually tested the democratic peace hypothesis. Most of the studies have focused on the mechanisms (see next section, caveat 2), and hence seem to assume that there is a correlation between democracy and war. In this way, the majority of the studies—often unintentionally—reinforce the idea that democratic peace actually exists without testing this proposition. However, none of the studies that directly test the democratic peace hypothesis found strong evidence that democracy is the most important factor when explaining interstate war. All democratic peace studies have controlled for many possible alternative causes of the peace, such as economic development and growth, geographic distance and contiguity, power status, alliance ties, militarization and political stability. The findings show that it is not just democracy which explains war, not at all. Within this group of studies, which explicitly test the democratic peace hypothesis, four different types of findings can be detected. I will discuss those results more in-depth in the rest of this section.

First Result: There Is Correlation, but Other Explanations Are Significant Too

The first subgroup consists of scholars who stress the importance of democratic peace, despite the fact their own analyses have shown that other factors are statistically significant as well (Maoz and Russett 1993; Rousseau et al. 1996; Gleditsch and Hegre 1997; Beck et al. 1998; Ray 2013). For example, some studies (e.g. Rousseau et al. 1996) included alternative independent variables in order to test realist arguments. They tested whether the distribution of power determines decisions to use force, and measures each state’s military capabilities relative to its opponent. A state’s military capability is the average of three elements: number of troops, military expenditures and military expenditures per soldier. They found that this realist variable was strong, positive and statistically significant at the 0.001 level in their analyses (see, e.g., Rousseau et al. 1996: 522, Table 2). However, not only a state’s military capabilities appeared to be an important explanation for peace. In addition, wealth, growth, alliances and contiguity played a crucial role when explaining interstate war (see, e.g., Maoz and Russett 1993: 632, Table 1).11 Moreover, when other factors are included, the impact of democracy on the likelihood of international crises is even spurious (Maoz and Russett 1993: 632; Henderson 2002: 141, see also p. 3).12 Still, scholars in this group keep defending the democratic peace idea, despite the fact that their own analyses showed the significance of alternative explanations.

Second Result: Initially There Is Correlation, but the Impact of Democracy Is Spurious When Other Explanatory Factors Are Included in the Models

The second subgroup of scholars is far more radical. Based on their own analyses, this group concludes that the democratic peace link is a spurious one (Weede 1984, 1996; Barbieri 1996; Mousseau 2013; Gartzke and Weisiger 2014).13 Typically, efforts to demonstrate the spuriousness of the statistical democratic peace pointed to other factors that, when accounted for ‘properly’, eliminated or dramatically reduced the statistical significance of shared democracy. Hence, the studies in this second group did not find strong evidence for the democratic peace hypothesis anymore, once other explanatory factors were included in the models.14

One of the most convincing alternative explanations of peace between countries is that there is no democratic peace, but a capitalist peace instead. The settlement in Germany and Japan succeeded because of the establishment of capitalist peace. Because of economic support by the Americans, who encouraged free trade and offered trade opportunities in practice as well, the poorer economies in Europe and Japan would gain economically, resulting in ‘economic growth, prosperity, and, ultimately, free trade among most of the more technologically advanced economies’ (Rasler and Thompson 2005: 232). By establishing and expanding free trade, the incentives for war would quickly decrease among trading states, according to this approach. To prevent new interstate wars after World War II, the capitalist peace was a far more important factor than the American promotion of democracy and its political institutions.

The capitalist peace, or capitalist peace theory, also states that economic development accounts for both democracy and the peace among democratic nations. Economic development is a key factor to explain democracy (Lipset 1959; see also Hegre 2003; Weede 2004).15 Moreover, economic development also plays a role when explaining peace, and the presence of market-oriented economies in countries have a positive impact on both democracy in those countries and peace between them (Mousseau 2000, 2002, 2003, 2005, 2013; see also Hegre 2014). Democratic peace only exists when both democracies have high levels of economic development, when economic development is well above the global median.

In fact, the poorest 21% of the democracies studied, and the poorest 4–5% of current democracies, are significantly more likely than other kinds of political systems to fight each other (see, e.g., Mousseau 2005). Moreover, if at least one of the democracies involved has a very low level of economic development, then democracy cannot prevent war.16 Still, there is a pacifying effect of free trade and economic interdependence, which is more important than the effect of democracy, because the former affects peace both directly and indirectly, by producing economic development and ultimately, democracy (see Weede 2004).17

Capitalist peace is not the only alternative explanation. Shared interests in general, and political similarities in specific, can also be seen as an important second alternative explanation for war and peace between countries (Farber and Gowa 1995, 1997; Gartzke 2007; Gowa 1999; Henderson 2002). Democracies are not peaceful to each other because they are democratic, but rather because they are similar. So the difference of the scores of both countries also contributes to the conflict proneness of the dyad. If the difference in levels of democracy is big, then the chance of conflict is higher (cf. Oneal and Russett 1997: 281–282).

Many researchers have conflated both the conflict-dampening impact of joined democracy and the confict-exacerbating impact of political distance in the variables focusing on political systems, but as Errol A. Henderson (2002: 32) convincingly argued: ‘Fusing these two contrasting attributes in a single variable makes it difficult to distinguish between the competing processes’. Therefore, it is better to include an additional variable of ‘political dissimilarity’ in the model. Henderson (2002) was one of the first scholars who included this variable and measured it by taking the absolute value of the difference between the two states’ scores. His main variables were not only political similarity, but also geographic distance and economic interdependence, and he concluded that democratic peace is a statistical artefact which disappears when those other variables are taken into account. Political similarity clearly has a pacifying effect18 (see Werner 2000; Henderson 2002; Beck et al. 2004), and it is not democracy per se which is the decisive factor.19

Hence, the benefits of trade and trade interdependence are essential explanations, while democracy is spurious or at least subordinate (see also Rosecrance 1986; Weede 1984, 1996; Hegre 2000, 2014; Jervis 2002; Souva 2003; Rasler and Thompson 2005: 235; Mousseau 2000, 2002, 2003, 2005). Based on those studies, it is safe to conclude that democracy, on its own, is an unlikely cause of the democratic peace.

Third Result: There Is Correlation, but Other Explanations Are Much Stronger

This same point that democracy is just one of the explanations for peace (and not even a very important one) is also at the core of studies in the third subgroup. Scholars of this group keep arguing that there is support for the democratic peace hypothesis, and that the link is not spurious. In this sense, they are less radical than the second group of scholars, as they do not completely reject the value of democracy for peace. On the other hand, their own analyses have clearly shown that alternative factors—hence other factors than democracy or type of political system— are not only statistically significant but also more important when trying to explain interstate war (Bremer 1992; Gelpi 1997; Oneal and Russett 1999a, b; Reiter and Stam 2002; Peterson 2013; Caselli et al. 2015).

Theoretical arguments and empirical evidence suggest that democracy is not the most important factor, while war is more likely to occur between states that are geographically proximate, approximately equal in power, major powers, allied, economically advanced and highly militarized than between those that are not. Bivariate analyses of these factors in relation to the onset of interstate war over all pairs of states in the period from 1816 to 1965 have generally supported these associations. However, multivariate analyses revealed some differences. Stuart Bremer (1992), for example, showed that some factors are far more important than others. The existence of a dangerous, war-prone dyad can be best explained by the presence of contiguity, the absence of an alliance and the absence of more advanced economy. The absence of democratic polity and other factors (absence of overwhelming preponderance, and presence of major power) are less powerful. Overall, these findings suggest that our research priorities may be seriously distorted and that we should not focus too much on the perceived positive impact of democracy, but on other factors (such as alliances and economic factors) instead.

Fourth Result: There Is Correlation, but Only Under Certain Specific Conditions

The final subgroup of scholars argues that we cannot unconditionally accept the idea that democratic peace exists in general, so always and everywhere. Their statistical studies clearly showed that support for this hypothesis heavily depends on other factors. The chance of democratic peace depends not just on the specific historical period (Cold War or not; Gibler and Sarkees 2004; Siverson and Emmons 1991; Weede 1984), but also the stage of the conflict (beginning, duration or severity; see Bremer 1993; Bennett and Stam 1996; Reed 2000), and on the neighbourhood instability (extent of confict in the region; see Gibler and Braithwaite 2013; Gibler and Miller 2013). Despite the differences between the studies, there is one common finding in all studies: when explaining interstate war, we cannot just rely on the impact of democracy, as it is too much dependent on other factors.

Several scholars found strong evidence for the idea that democratic peace exists, but only during some specific historical periods. Based on this evidence, they concluded that democratic peace is simply a statistical artefact of the Cold War. For example, Henry Farber and Joanne Gowa (1995) found statistical support for the idea that peace between democracies is an artefact of the Cold War, when the threat from the communist states forced democracies to ally with one another (see also Mearsheimer 1990). Sebastian Rosato (2003) also argued that most of the significant evidence for democratic peace has been observed after World War II; and that it has happened within a broad alliance, which can be identified with NATO and its satellite nations, imposed and maintained by American dominance.

Since the Second World War, war has become a very costly affair. Scholars discovered that only a handful of states are ‘capable of engaging in major power warfare. That process of elimination has not yet extinguished the possibility of major power warfare, but it has lowered its probability immensely’ (Rasler and Thompson 2005: 219). The chance to achieve something in a war is low in general, and even lower in a bipolar world with two big power players risking high nuclear war costs (Jervis 2002). While war became more costly, trade became less costly; as a consequence, the war/trade costs increased during the Cold War (Rosecrance 1986; see also Jervis 2002). In such a world, war and conflict have become less attractive, while trade and cooperation have become more appealing (Rasler and Thompson 2005: 219). Hence, more states decided to adopt trading strategies in order to prevent confict and war as much as possible. In the end, democracy was part of the story, but only a very small part with a subordinated role next to the power dynamics during the Cold War, the costs of warfare and the benefits of trade.

Some scholars found evidence that the democratic peace still exists in the post-Cold War period (Park 2013) which weakens this argument. However, most analyses showed that dyadic dispute rates have converged after the Cold War (see, e.g., Gowa 2011). Moreover, jointly democratic dyads are likely to be allied only after 1945 (see Gibler and Sarkees 2004); during the 1816–1944 time period, there is even a negative relationship between democratic dyads and alliance formation.20 These findings cast serious doubts on the idea of a general existence of democratic peace.

Not only the historical period, but also the *stage* of the conflict is crucial. Some scholars in this group provided evidence that democratic peace is not universal, but that it depends on the stage and whether we focus on the beginning, duration or severity of the conflict. Although joint democracy has some pacifying effects on the onset of conflict, the results suggest that they are unrelated to the escalation of disputes to war (see Reed 2000). Moreover, democratic peace is dependent on the neighbourhood instability. Democracies often have few territorial issues over which to contend, as they tend to be part of a stable region. Democracies only seldom have territorial disputes with their neighbours, and therefore they can more easily choose favourable conflicts to escalate. The type of political system does not predict conflict selection or victory once controls are added for issue salience (Gibler and Miller 2013; see also Park and James 2015). There is an interaction between joint democracy and regional instability, which confirms the idea that the effects of type of political system on continued conflict apply mostly to dyads in peaceful regions (Gibler and Braithwaite 2013; see also Park and James 2015). Very democratic countries might even become more aggressive and faster than other political systems, once the region becomes more hostile (see, e.g., Baliga et al. 2011).

The General Lesson from the Results in a Nutshell (Caveat 1)

In short, regardless of the differences between the statistical studies on democratic peace, all findings have indicated that other explanations are important as well. It is clear that democracy is just one of the explanations, and certainly not the most important one,21 sometimes even spurious and often heavily dependent on other factors. It is not (just) democracy to be preoccupied with, when trying to prevent war between countries (Table 3.1).

Caveat 2: What Are the Causal Mechanisms?

Most of the statistical studies on democratic peace seem to assume that there is a correlation between democracy and war; based on this assumption, they then decide to focus on the mechanisms. This is problematic as none of the democratic peace studies found strong evidence that democracy is the most important factor when explaining interstate war (see the previous section). As a consequence, the next step of looking for mechanisms is quite irrelevant and not necessary in my view, but most studies nevertheless argue that the field lacks strong theoretical foundations and robust empirical evidence that can reveal convincing causal mechanisms.22 Those studies seem to accept the correlation between dyadic democracy and peace, and then start questioning whether democracy really causes peace before investigating potential mechanisms.

Table 3.1 Statistical studies on democracy and interstate war (dyadic level)

|  |  |
| --- | --- |
| Caveat 1: It’s Not (Just) Democracy | Studies |
| ‘It’s just democracy; democracy is most important explanation for peace between countries’ | No studies found |
| ‘There is correlation, but other explanations are significant too’ | Beck et al. (1998), Gleditsch and Hegre (1997), Maoz and Russett (1993), Ray (2013), and Rousseau et al. (1996) |
| ‘Initially there is correlation, but the impact of democracy is spurious when other explanatory factors are included in the models’ | Barbieri (1996), Beck et al. (2004), Farber and Gowa (1997), Gartzke (2007), Gartzke and Weisiger (2014), Gowa (1999), Hegre (2000, 2003, 2014, Jervis (2002), Mousseau (2000, 2002, 2003, 2005, 2013), Oneal and Russett (1997), Rasler and Thompson (2005), Rosecrance (1986), Souva (2003), Weede (1984, 2004), and Werner (2000) |
| ‘There is correlation, but other explanations are much stronger’ | Bremer (1992), Caselli et al. (2015), Gelpi (1997), Oneal and Russett (1999a, b), and Peterson (2013) |
| ‘There is correlation, but only under certain specific conditions’ | Baliga et al. (2011), Bremer (1993), Bennett and Stam (1996), Farber and Gowa (1995), Gibler and Braithwaite (2013), Gibler and Miller (2013), Gibler and Sarkees (2004), Gowa (2011), Jervis (2002), Mearsheimer (1990), Park (2013), Park and James (2015), Rasler and Thompson (2005), Reed (2000), Rosato (2003), Rosecrance (1986), Gibler and Sarkees (2004), Siverson and Emmons (1991), and Weede (1984) |

### AT: Demo ! – Collective Action

#### Democracy fails to overcome collective action problems – populism and other self-defeating aspects are endemic, NOT backsliding

Di Paola 18 Marcello Di Paola, Postdoctoral Researcher in Philosophy at the University of Vienna, and Research and Teaching Fellow at LUISS University in Rome; and Dale Jamieson, Professor of Environmental Studies and Philosophy, Affiliated Professor of Law, and Affiliated Professor of Medical Ethics at New York University; “Climate Change and the Challenges to Democracy,” University of Miami Law Review, 72(2), 3-9-2018, <https://repository.law.miami.edu/cgi/viewcontent.cgi?article=4528&context=umlr> /GoGreen! \*added [halt]

VI. THE INTERLOCKING CRISES

In this Part, we highlight how the vulnerabilities of democracy are made salient as well as exacerbated by climate change and other problems of the Anthropocene. We also emphasize how climate change and other problems of the Anthropocene place democracies that attempt to navigate them in a particularly impervious Scylla and Charybdis-like situation.173 The Scylla is ineffective policy; the Charybdis is some relaxation of the core democratic principle of popular sovereignty. Both options seem nearly guaranteed to trigger significant legitimacy challenges to liberal democratic systems.

Traditionally, two important sources of democratic legitimacy have been beneficial consequences, in the utilitarian tradition, and consent, in the social contract tradition.174 Whatever else may count as beneficial consequences, the capacity to solve problems that threaten the physical and social security of citizens is a central and important source of democratic legitimacy.175 Call this the “public utility” view of democratic legitimacy. And whatever else may count as consent, surely the fact that the majority of citizens have expressed their preference for a certain candidate, law, or policy is an important source of democratic legitimacy as well.176 Call this the “expressed preference” view of democratic legitimacy.

Consider public utility first. As we have pointed out, most contemporary democracies have thus far failed to address the emerging problems of the Anthropocene.177 Consequently, the sense of physical and social insecurity grows more acute amongst citizens as the problems mount and compound.178 The legitimacy of these democracies, and the supranational institutions they have created, such as the European Union and the United Nations, is thus compromised on public utility grounds.

Now consider expressed preference. The global scope, long-term reach, unprecedented features, and highly complex nature of climate change and other problems of the Anthropocene require democracies to make robust commitments to multilateral cooperation, long-term planning, significant deviations from the status quo, and increased reliance on expert knowledge if they are to succeed in managing these problems. 179 Citizens’ expressed preferences may be quite distant from this network of commitments and activities,180 since the benefits of successfully managing a problem like climate change would mostly accrue not to these citizens, but to spatiotemporally distant people (i.e., the global poor and future generations) and genetically distant (non-human) nature. 181 Attempting to force such commitments, especially at a time when democracies are already being accused of not being responsive enough to their citizens, can further compromise legitimacy.182

We thus face an apparent dilemma: if democracies fail to successfully address climate change and other problems of the Anthropocene, their legitimacy will be challenged on public utility grounds. If they aggressively attempt to address them, their legitimacy will likely be challenged on expressed preference grounds. Either way, we can expect the power of populist figures and movements to grow.

The remainder of this Part illuminates this dilemma by discussing how climate change and other problems of the Anthropocene interact with some further democratic vulnerabilities: weak multilateralism, short-termism, the profusion of veto players, the contested role of experts, and self-referring decision making.

A. Weak Multilateralism

Climate change cannot be successfully managed without a strong commitment to international cooperation.183 For a climate regime to succeed, it must be effective, perceived as at least not unfair by all parties, and otherwise acceptable to each party.184 At various times, the attempt to create a regime has foundered on each of these three considerations.185

From the beginning of the negotiations that led to the adoption of the FCCC in 1992 and in subsequent negotiations under the Convention, the question of fairness has been unavoidable.186 When agreements have been structured in ways that are acceptable to developing countries (e.g., the Kyoto Protocol) they have been perceived as unfair by the United States.187 This has led to the weakening of commitments and to a regime whose effectiveness is in question.188 The Paris Agreement, by putting voluntary pledges at the center, was designed to avoid the problem of perceived unfairness.189 It was reasonably thought that no party could say that they had been unfairly treated when they have agreed to be measured in relation to a commitment that they have voluntarily undertaken and to which no sanctions are attached for non-compliance. 190 Nevertheless, that was exactly the claim made by President Trump in announcing his intention to withdraw the United States from the Paris Agreement.191 Moreover, the cost of creating an agreement to which no one could reasonably object was to create an Agreement whose effectiveness was in question even before the United States announced its intention to withdraw.192

While climate change is its own “full tragedy and weird comedy,” 193 there are structural issues at work.194 As the world order attempts to adjust to shifting power distributions following the emergence of new giants such as China and India, when it comes to problems such as climate change the cooperation of such countries is no longer just desirable but essential.195 As their collaboration becomes more valuable, the price for obtaining it rises accordingly.196 This complicates negotiations, and the problem seems only destined to worsen because this logic applies not only to presently emerging world powers, but also to those that have already emerged and those that will emerge in the future. As we observed in an earlier paper, “[g]lobal governance in the Anthropocene is cooperation-hungry, and this increases the price of obtaining cooperation from every country.”197

In addition, democracies have their own particular problems when it comes to multilateral agreements. Except in the rare case where they are able to steer multilateral agreements in the way they prefer, democratic governments “often seek to avoid compliance with binding multilateral decisions if this weakens their relationship to their electorate.”198 This is in fact what happened in the case of President Trump’s repudiation of the Paris Agreement.199 The stated reason was the agreement’s unfairness to the United States.200 However, the deeper reason was that the Obama administration’s decision to join, although admittedly an act of national self-determination, was not in fact an authentic deliverance of American popular sovereignty, at least in the eyes of Trump and his supporters.201 According to Trump,

[t]he Paris Climate Accord is simply the latest example of Washington entering into an agreement that disadvantages the United States to the exclusive benefit of other countries, leaving American workers – who [sic] I love – and taxpayers to absorb the cost in terms of lost jobs, lower wages, shuttered factories, and vastly diminished economic production.202

In the same speech Trump reminded his audience that “I was elected to represent the citizens of Pittsburgh, not Paris.”203

In democracies, it is ultimately citizens who empower their representatives to bargain and strike terms of international cooperation.204 Successfully addressing the problems of the Anthropocene is likely to require unprecedented levels of multilateralism.205 Democratic states that attempt to rise to the challenge are likely to face legitimacy challenges on expressed preference grounds. Those that do not may face legitimacy challenges on public utility grounds.

B. Short-termism

Short-termism can be defined as “the priority given to present net benefits at the cost of future ones.”206 Short-termism is a problem whenever policy domains have an extended timeframe, as is the case with climate change and other systemic problems of the Anthropocene.207 In these cases, present net benefits may need to be curtailed (through increases in taxes and regulations, for example) for the sake of benefits that might materialize in the distant future. These future benefits will then mostly advantage people other than those who have borne the costs. Reasons for privileging the present in these cases include pure time preference, uncertainty, and diminished or even null moral concern for those who might benefit in the future.208 The temptation, then, is to eschew the costs of the required policies and “pass the buck” to future generations.209

Short-termism is not always irrational nor morally wrong.210 It has been argued, however, that short-termism is both irrational and morally wrong in the case of climate change.211 The sources of short-termism are rooted in human psychology and can manifest in any kind of political regime.212 However, it has been argued that democracies are particularly vulnerable to short-termism.213

One important reason for the short-termism of democratic political regimes is that these regimes inherit, via voting and other forms of popular influence, their citizens’ biases in favor of the present. Policies may also reflect citizens’ misinformation about, or unawareness of, long-term processes, risks, policy aims, and possible outcomes.214 To counter these tendencies, liberal democracies typically filter their citizens’ inter-temporal biases, misinformation, and unawareness through such mechanisms as constitutions and reliance on expert bodies.215 Yet the more filtering they do, the more likely they are to incur legitimacy challenges on expressed preference grounds.216 This is a problem of intra-generational legitimacy.217

There are also problems of inter-generational legitimacy.218 There is no guarantee that long-term policies, if enacted, will achieve the anticipated aims, or that they will indeed make future people better off by achieving these aims.219 If things do not work out, these policies might be deemed illegitimate on public utility grounds by the very future people that they were supposed to benefit.220 In addition, such policies may be deemed illegitimate by future people on expressed preference grounds.221 Legitimacy on expressed preference grounds typically requires some form of authorization by those who are affected by policies, yet future people who will be affected by past policies never authorize them, nor can they hold anyone accountable.222

Another reason for democracies’ short-termism is the scheduling of participatory events.223 Democracy requires elections, which must be relatively frequent in order to ensure that people can regularly express their will, vote out politicians who are judged to have failed in some important ways, and prevent rent-seeking behavior by not giving politicians enough time to set up camp within institutions.224 However, the relatively short duration of electoral cycles ensures that politicians are constantly concerned with their own reelection, and this may prevent them from taking hard policy decisions that require a great deal of political capital and do not produce appreciable outcomes in time for the next election.225 Because most of the impacts of climate change will largely materialize in the future and be felt by future generations, efforts at their alleviation must obey a clock that is not in sync with the electoral clock.

Note that there is no need to assume that politicians are always and necessarily motivated by only a thirst for power.226 In a democ- racy, even politicians who are exclusively motivated by the aspiration to make good long-term policy need to be elected or re-elected to do so.227 In order to be elected, they need to harness the votes of the current electorate.228 So, the problem of short-termism goes beyond a lack of conscientious far-sightedness on the side of politicians: it is structurally connected to the very fact of popular sovereignty—at least as long as the majority of people discount the future.229

C. Veto Players

Any political system (with the possible exclusion of some forms of anarchy) accords veto powers to some agent: a monarchy to the king, an aristocracy to the nobility, a technocracy to the experts, a theocracy to the religious leader, and so on.230 A veto player in a political system can be understood as an agent who can prevent a departure from the status quo.231 In democracies, veto players can be specified by constitutions (e.g., the President and the Congress in the United States), emerge from the political system (e.g., the Supreme Court in the United States, political parties that are members of a government coalition in Western Europe), or from civil society (e.g., powerful industries, unions or other interest groups in many countries).232

In a democracy, veto players can protect minority interests, prevent destabilizing change, and preserve important values and policies through periods in which they are unpopular.233 More generally, veto players prevent a democratic system from being excessively fluid and flexible.234 This is attractive when the status quo is desirable or an exogenous shock is beneficial; however, when the status quo is undesirable or an exogenous shock disturbs a desirable status quo, fluidity and flexibility are needed in order to respond quickly

and decisively.235 This is arguably the situation in the case of climate

change, which demands nimble political responses to which veto

players would have to acquiesce.

The presence of many veto players threatens to delay or even block the formulation and implementation of policy.236 Liberal democracies, with their reliance on checks and balances generated by institutional architecture or by competition among interest groups, seem particularly vulnerable to such threats—and the more veto players in a democracy the greater the degree of vulnerability.237

An especially high concentration of veto players helps to explain why a powerful, rich, technological leader like the United States is uncannily slow to address consequential public issues such as the politics of distribution, racial equality, immigration, the proper balance between liberty and national security, and of course climate change.238 The United States Constitution separates powers in the federal government, reserves a broad range of powers to states and includes a bill of rights that can be viewed as effectively giving veto powers to individuals in some circumstances. Practices have also developed through time that inhibit action, such as requiring supermajorities for some political decisions.

The profusion of veto players may be extreme in the United States, but it is a feature common to many liberal democracies that often makes political action elusive even on relatively minor policy issues.239 For every possible policy change, there is always a “do-nothing” alternative (sometimes more respectably presented as a “wait and see” alternative) that is invariably attractive to some veto player.240

“Do-nothing” alternatives may sometimes be justified on grounds of rational choice considerations relating to transition costs and uncertainty about both the process of transition and the final pay-off structure.241 Veto players give voice to such considerations, as well as other considerations that we have already noted.242 But veto players may also give voice to less rational tendencies, which are inevitably present and, in democracies, are crystallized in votes. Among these tendencies may be disproportionate attention to sunk costs, finding refuge in “what has always worked,” fear of regretting the changes made, the desire to maintain and transmit a sense of control by not acceding to the demands of new circumstances, and lack of trust in those who are proposing the changes.243

Veto players tend to slow down or block deviations from the status quo, and this makes it difficult to tackle climate change and other similar problems of the Anthropocene.244 But veto players also reflect and configure real structures of power, and protect and promote the needs and interests of actual people.245 When the number of veto players or the importance of specific veto players is altered, new power structures emerge and this can raise legitimacy challenges on both utility and expressed preference grounds.246 It is not obvious what veto players should be eliminated or demoted in order to produce more nimble and effective climate policy, and which ones should be given additional power instead. Nor is it obvious who should decide the answers to these questions (if not the people) and on what grounds (if not majority rule).

Veto players configure systems of checks and balances, filters and buffers, which are only partially exposed to popular influence.247 This anti-majoritarian service is particularly precious to liberal democracies, which rely on veto players to protect and promote the rights of individuals and minorities—and, with that, the core liberal principles of individual liberty and human rights. However, as a consequence, if a majority exists that is overwhelmingly convinced by climate science, totally in favor of leaving all remaining fossil energy sources in the ground, and ready to embark on ambitious renewable energy programs, this majority may still find it difficult to act. Liberal democracies protect minorities of various kinds in varying degrees, and these include climate change denialists and those who profit from fossil fuels. Economically powerful and en- trenched economic minorities (the “1%”) are often extremely effective veto players.248 This can prevent action that would benefit most people, thus increasing the risks of legitimacy challenges.

D. Contested Role of Experts

Climate change and other problems of the Anthropocene are unprecedented phenomena whose complexity and implications are only beginning to be understood by scientists and other experts. Climate change is a multidimensional problem that concerns and connects ecology, demography, development, production, consumption, resource use, trade rules, health, security, urban planning, mobility, migration, and more, in novel ways.249 It poses threats that are multi-scalar, probabilistic, indirect, often invisible, spatiotemporally unbound, and potentially catastrophic. These threats challenge our reason, emotions, and imagination.250 If there were ever a complex problem that required expert knowledge, it is climate change.

Liberal democracies make significant use of expert knowledge in policymaking in various ways to protect liberal values, and to boost their efficiency, equity, and political stability.251 Expert knowledge is distinguished from non-expert opinion through such criteria as experience, professional and educational qualifications, peer-review, and rules of evidence.252

Still, in a democracy, differences in expertise do not translate to differences in political authority, for much the same reason why differences in lineage do not translate in this way. A democratic citizen can recognize expertise and accept the science of, say, climate change, and still object to the expert who counsels some course of action: “You may be right, but who made you boss?”253 In a democracy, expertise is always subservient to the voice of the people (pace Plato, philosophers cannot be kings).254

For this reason, the relationships between experts and ordinary citizens are always potentially fraught in a democracy. These relationships vary from country to country, time to time, and issue to issue. Often, the relationships are placid in good times and rocky in hard times. Major policy failures, such as the global financial crisis of 2008 and the spreading of terrorist radicalization in many European Union countries, can lead citizens to question experts’ knowledge and see them as just another interest group seeking rents at people’s expense.255

In the case of climate change, an additional element makes the role of experts potentially unpopular. Climate science, in our present social context, inevitably provokes fundamental questions about how we ought to live and organize our societies, throwing doubt on the ways in which we do so now. A particularly powerful and widespread attempt to avoid cognitive dissonance through various forms of rationalization may thus come into play. After all, if something potentially catastrophic such as climate change can result from the very ways in which we live our everyday lives—how we dwell, how we eat, how we make things, how we move around—the nagging thought is that there might be something fundamentally wrong about the ways in which we live. These are not comfortable thoughts and can lead to resentment or worse towards those who bear the message.

The incipient conflict and simmering resentment has been exploited by powerful interests who look to be the immediate losers from a transition to a more sustainable way of life. They stoke the dissonance and encourage denialism. The most obvious manifestation of this is the climate change denial campaign, directed towards preventing the formation of a consensus for political action on climate change.256

The main strategy of climate change denialists has been to suppress both belief in the science and belief that there is a scientific consensus on the existence, anthropogenic nature, and dangerousness of climate change.257 In its aims and strategies, climate change denialism has replicated earlier forms of denialism involving tobacco smoking, acid rain, DDT, and ozone depletion. 258

The rhetorical techniques adopted by climate change denialism have also not been particularly original: versions of these techniques were used in all the other cases mentioned above. These techniques include attacking sources rather than discussing evidence, “moving the goalpost” by requesting ever larger amounts of evidence, submitting false evidence, suggesting false equivalences or analogies, confusing ignorance about mechanisms or processes with ignorance about facts or outcomes, cherry-picking anomalies, selective skepticism, quote mining, and the so-called “Gish gallop”—overwhelming discussants or audiences with unscientific claims to make it difficult to counter all the misinformation at once.259

What is new about denialism in the Anthropocene is not its strategies or tactics, but its amplification. Expertise denialism now travels through social media, which allows for unfiltered instant communication among citizens and between citizens and representatives. Traditional intermediaries—political parties, intellectuals, and the professional press—are increasingly made redundant by these technologies. Indeed, to maintain their relevance (and market share), these traditional intermediaries often seek to replicate the immediacy and excitement of social media, compromising their own claims to epistemological or institutional privilege.

One effect of the speed and directness with which political communication occurs through social media is an increased tendency to brand political ideas and policy proposals and to market them as products.260 The need to engage audiences with arguments and relevant facts—and even to maintain consistency in one’s opinions— decreases, while the need for a good, resonant, quick-win pitch increases. With that, the importance of expert knowledge is downplayed to the advantage of skilled branding and marketing.

Another effect of the speed and directness with which political communication occurs through social media is a polarizing fragmentation, not just at the level of policy judgments, but also regarding the sets of facts to which different individuals and groups make reference. Social media allows for networked, yet highly fragmented, political communication, making it harder to individuate and even debate a common story.261

Much empirical work in psychology, economics, political science, sociology, and communications has gone into trying to explain how and why disagreement about facts can occur.262 The explanation seems to be some sort of “biased assimilation,” whereby people adjust their view of facts with reference to their self-defining values, social identities, and partisan allegiances.263 Experiments on reception suggest that individuals selectively credit or dismiss information in a manner that reinforces beliefs congenial to their values.264 These experiments found that subjects were substantially more likely to count a scientist as an authoritative “expert” when the scientist was depicted as taking a position consistent with the subjects’ cultural predispositions, than when that scientist took a contrary position.265 Interestingly, these tendencies seem to be directly, rather than inversely, related to levels of science literacy and general education of experimental subjects: the more equipped people are to know and understand the facts, the more they disagree on them.266

In times of social media, these tendencies may be amplified, insofar as individuals tend to gravitate towards and engage mostly with resonant networks of “like-me’s” that by and large reaffirm their own values and perspectives.267 This may tribalize positions and impede constructive democratic engagement and debate from ever taking off on many contested issues. In addition, one can expect increasing polarization to also be fomented by individuals and groups trying to secure loyalty to their branded political ideas and policy proposals in this way.

The internet and other media, with their seemingly endless resources, create the impression that expertise can be picked and chosen at will, thereby feeding the perception of public life as a spectacle.268 Public discussions, unfiltered by “moderators,” unfold in a denuded space stripped of epistemological norms.269 In the United States at least, this has morphed into a generalized atmosphere of expertise denialism writ large. Denialism about evolution, vaccines, economics, and more has become commonplace.270

It is not an exaggeration to say that we are on the verge of adopting epistemological nihilism as a public epistemology.271 No commitment to facts, in the traditional sense, or even consistency of opinion, is required.272 Truth is what the speaker says it is, here and now. In a moment it may be different, depending on what the speaker can get away with. In a democracy, it is up to elections or approval ratings to resolve disagreements. It is a short step from here to other exercises of power.

The nihilistic turn in public epistemology threatens the legitimacy of democracy, for democracy cannot solve the problems it faces without mobilizing epistemological authority that is itself hostage to popular vote. As difficult as this challenge may be in favorable times, it is greatly magnified in the face of climate change and other problems of the Anthropocene.

E. Self-referring Decision-making

What we have elsewhere called the “agency presupposition” is deeply entrenched in modern democratic theory. This presupposition holds “that the political community is constituted by agents who initiate and conduct political action, and who themselves, and their interests and welfare, are what matter politically.”273 The agency presupposition arose at a time in which democratic principles, norms and institutions were being developed to govern relations between agents who lived in close proximity to one another in space and time, and whose decisions and actions had relatively direct impacts on each other. However, around 1950, a profound change occurred from a world of discrete but interdependent states to a world of shared social space in which distant events have localized impacts and vice-versa. In this globalized world, the fates of nation-states and their peoples became not just effectively interdependent, but also structurally interconnected, with social, political, and economic activities, interactions, and infrastructures stretching beyond political frontiers, leading to a deepening enmeshment of the local and the global.274 Political decisions and actions taken locally (in selected powerful countries, many of which were democratic) now systematically had planetary implications, impacting for better or worse the welfare and interests of people in all corners of the world.

With the Anthropocene disruption of earth’s fundamental ecological systems, including those that govern climate, political agents (living humans who can initiate and conduct political action) have gained unprecedented power over a vast universe of non-agents that comprises animate and inanimate nature as well as those living on the periphery of both space and time.275 The circle of affected nonagents has expanded beyond cultural, genetic, and spatiotemporal boundaries to include virtually everything on the planet, now extended indefinitely in time.276 This establishes an enormous asymmetry of power. Those on the periphery, and nature, cannot initiate and conduct political action: they cannot reciprocate, they cannot participate, they cannot protest, they cannot retaliate.277 In democratic terms, they do not matter—or only matter derivatively, if political agents care about their fate. And it is as undemocratic as can be, particularly if the democracy in question is a liberal democracy, to force political agents to care if they do not.278

A phenomenon like climate change creates ubiquitous tensions and trade-offs between agents and non-agents—those who are governed, and those who are affected.279 The latter will suffer most from climate change, but a democracy responsive to the claims of future generations (or those living beyond its borders, or nonhuman nature) may often have to forgo opportunities for bringing beneficial consequences to those who empower it with their votes.280 Instead, democratic leaders would have to enact policies favoring the interests of those who do not vote because they do not yet exist (or live in different countries or are not human).

Democracies making policies that favor non-agents will expose themselves to intra-generational legitimacy challenges on both public utility grounds and expressed preference grounds.281 Even if the expected benefits to non-agents were great, such non-agent-oriented policies might not win the hearts, minds, and guts of living human agents who may express their preference for themselves instead— particularly in democracies that are already being accused of not being responsive enough to their citizens.282 Many believe that ignoring or heavily discounting the welfare and interests of non-agents is morally wrong, but if expressed preference is important, it may be a wrong that democracies cannot avoid committing.283

The agency presupposition makes government responsive to those who are governed but not to those who are affected beyond borders in space, time, citizenship, or genetic make-up. A basic presupposition of liberal democracy appears to be threatened by the very actions that would have to be taken to express concern for all those affected by the climate-changing and eco-altering actions of its citizens.

VII. CONCLUSION

We began this Article by explaining the notion of the Anthropocene and briefly telling the story of failed responses to climate change. We went on to discuss the uneasy relationship between climate change and democracy, focusing on liberal democracy in particular. We presented some basic aspects of democratic theory and practice, and discussed some of democracy’s main vulnerabilities. We showed how in the Anthropocene these vulnerabilities can magnify, leading to legitimacy challenges.

These legitimacy challenges are not new. Democracy has always been haunted by anxiety about its future. Some political theorists have argued that democracy is the only form of political organization that underwrites the seeds of its own destruction.284 Demagogues and extremists who wish to blow up the state are allowed the same freedoms as those who seek to manage it more fairly and effectively. The risk of a democratically enabled democide is not an abstract or counterfactual risk: the executioners of German democracy came to power through the rules and procedures of the Weimar Republic.285 If we open our eyes, we may see these stories going on around us today.

Modern democracy is, in many respects, the most sophisticated articulation of the human capacity for social organization. It is also the most hospitable environment for the expression of human values that, through centuries of emancipatory struggles, have come to be regarded as fundamental, such as individual liberty and political equality.286 Our objective in this Article is not to write a requiem for democracy, but rather to chart the seas that democratic theory and practice will have to navigate in order to successfully address climate change and survive the challenges of the Anthropocene. We have highlighted the vulnerabilities of democracy in order to throw in sharp relief the many challenges entailed by the voyage, not to discourage it. Democracy has shown itself to be remarkably resilient in the past, and it may well succeed in rising to these challenges as well. There are those who think that democracy doesn’t stand a chance.287 But many still believe that the only solution to the problems of the Anthropocene lies in more, better, or different democracy.288 And there are those who think that even if democracy fails these challenges, democracy itself will not have failed. For they see its value as intrinsic, and not just as a means to better or more effective governance.289

It is difficult to sketch the nature of possible democratic solutions to some of the issues that we have raised, and we will not try to do so here. Instead, we will close with a summary of what seems to be the main challenge ahead. The existing democratic deficits in liberal countries will generally have to be reduced. Yet, in the case of climate change and other problems of the Anthropocene, liberal democratic countries will have to muster both the internal coherence and strength to better resist populism, and the external coherence and strength to be more cooperative partners within the framework of supranational institutions. This is necessary because, in the Anthropocene, the global spills into the domestic and vice-versa: a globally changing climate may have pernicious local impacts on the territory and population of any given country, while political dysfunction in one country can cripple [halt] efforts at global governance.

The democracies of the Anthropocene will have to work at multiple scales in both space and time, incorporating the interests of the global with those of the local, and those of the future with those of the present. This seems to suggest, perhaps paradoxically, that the democracies of the Anthropocene will have to be more democratic in some respects and less democratic in others. The relation between popular sovereignty and institutions that limit popular sovereignty while respecting it is a tug-of-war in democratic theory and practice that has been going on for millennia, and is now being put to unprecedented tests.

Liberal democracies, in particular, have an enormous amount at stake. Liberal political theory has always recognized the right to resist and even overthrow illegitimate political power.290 This right has been used to justify historical events that liberals typically applaud, including the Glorious Revolution, the French Revolution, and the American Revolution.291 Despite their failures and excesses, these revolutions forwarded liberal values and helped to entrench them in institutions. Unable to find consistent responses to challenges to their own legitimacy in the Anthropocene, liberal democracies may be in danger of warranting revolutions against themselves and the very institutions that should realize their values. They may become the ancient regime.

### AT: Terror !

#### No nuclear terror and no impact

John Mueller & Mark G. Stewart 21, Mueller is Woody Hayes Senior Research Scientist, Mershon Center for International Security Studies, and adjunct professor of Political Science, at Ohio State University, also a Senior Fellow at the Cato Institute in Washington; Stewart is Professor of Civil Engineering and Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia, “Terrorism and Bathtubs: Comparing and Assessing the Risks,” Terrorism and Political Violence, vol. 33, no. 1, 01/02/2021, pp. 138–163

The likelihood that anyone outside a war zone will be killed by an Islamist extremist terrorist is extremely small. In the United States, for example, some six people have perished each year since 9/11 at the hands of such terrorists—for an annual fatality rate of about one in 50 million for the period.

This might be taken to suggest, as one writer has characterized it, that “terrorism is such a minor threat to American life and limb that it’s simply bizarre—just stupefyingly irrational and intellectually unserious—to suppose that it could even begin to justify the abolition of privacy rights as they have been traditionally understood in favour of the installation of a panoptic surveillance state.” 1 And terrorism specialist Marc Sageman characterizes the threat terrorists present in the United States as “rather negligible.” 2 The vast majority of what is commonly tallied as terrorism has occurred in war zones, and this is especially true for fatalities.3 But even this has been exaggerated by conflating terrorism with war: civil war violence that would previously have been seen to be acts of insurgency are now often labeled terrorism.4

In order to put the numbers in some context, it has often been pointed out that far more Americans are killed each year not only by such highly destructive hazards as drug overdoses or automobile accidents, but even by such comparatively minor ones as lightning, accident-causing deer, peanut allergies, or drowning in bathtubs. Some comparisons are arrayed in Table 1.

In recent years, however, critics have attacked what they call “the bathtub fallacy.” 5

First, they stress that it is important to keep in mind that bathtubs are not out to kill you while terrorism is a willful act carried out by diabolical, dedicated, and clever human beings. Thus, although the number of people Islamist terrorists have been able to kill in the West since 9/11 has thus far been quite limited, those terrorists, as they plot and plan and learn from experience, may very well become far more destructive in the future.

Second, the critics charge that the comparison of terrorism with bathtub drownings is incomplete in that it doesn’t consider the possibility that the incidence of terrorist destruction is low precisely because counterterrorism measures are so effective.

Third, it is argued that, unlike bathtub drownings, terrorism exacts costs far beyond those entailed in the event itself. It damagingly sows terror, fear, and anxiety; disturbs our

Table

Description automatically generated

psychological well-being; undermines trust and openness within the society; and reduces our sense of intrinsic moral worth even as it increases a sense of helplessness. They maintain, fourth, that the comparison is invalid because, unlike terrorism, bathtubs provide benefit.

And finally, they contend that terrorism costs are peculiarly high, particularly in a democratic society, because the fears it generates will necessarily need to be serviced by policy makers, and this pressure forces, or inspires, them to adopt countermeasures, both foreign and domestic, that are costly and sometimes even excessive.

In this article, we examine these five propositions and find all of them to be wanting. In the process, we conclude that terrorism is rare outside war zones because, to a substantial degree, terrorists don’t exist there. In general, as with rare diseases that kill few, it makes more policy sense to expend limited funds on hazards that inflict far more damage.

Terrorism is willed and may well become more destructive

Journalist Jeffrey Goldberg has suggested that “the fear of terrorism isn’t motivated solely by what terrorists have done, but what terrorists hope to do.” Bathtubs are simply not “engaged in a conspiracy with other bathtubs to murder ever-larger numbers of Americans.” However, terrorists “in the Islamist orbit,” he insists, “seek unconventional weapons that would allow them to kill a far-larger number of Americans than died on Sept. 11.” 6 Or as Janan Ganesh of the Financial Times puts it, “Bathroom deaths could multiply by 50 without a threat to civil order. The incidence of terror could not.” 7

Thus far, 9/11 stands out as an extreme outlier: scarcely any terrorist act, before or after, in war zones or outside them, has inflicted even one-tenth as much total destruction. That is, contrary to common expectations, the attack has thus far been an aberration, not a harbinger.8 And al-Qaeda central, the group responsible for the attack, has, in some respects at least, proved to resemble President John Kennedy’s assassin, Lee Harvey Oswald—an entity of almost trivial proportions that got horribly lucky once. The tiny group of perhaps 100 or so does appear to have served as something of an inspiration to some Muslim extremists. They may have done some training, may have contributed a bit to the Taliban’s far larger insurgency in Afghanistan, and may have participated in a few terrorist acts in Pakistan. In his examination of the major terrorist plots against the West since 9/11, Mitchell Silber finds only two—the shoe bomber attempt of 2001 and the effort to blow up transatlantic airliners with liquid bombs in 2006—that could be said to be under the “command and control” of al-Qaeda central (as opposed to ones suggested, endorsed, or inspired by the organization), and there are questions about how full its control was even in these two instances, both of which, as it happens, failed miserably.9 And, although some al-Qaeda affiliates have committed substantial damage in the Middle East, usually in the context of civil wars, their efforts to carry out terrorism in the West have been rare and completely ineffective.10 Even under siege, it is difficult to see why al-Qaeda could not have carried out attacks at least as costly and shocking as the shooting rampages (organized by other groups) that took place in Mumbai in 2008 or at a shopping center in Kenya in 2013. Neither took huge resources, presented major logistical challenges, required the organization of a large number of perpetrators, or needed extensive planning.

However, there is of course no guarantee that things will remain that way, and the 9/11 attacks inspired the remarkable extrapolation that, because the terrorists were successful with box cutters, they might soon be able to turn out weapons of mass destruction— particularly nuclear ones—and then detonate them in an American city. For example, in his influential 2004 book, Nuclear Terrorism, Harvard’s Graham Allison relayed his “considered judgment” that “on the current path, a nuclear terrorist attack on America in the decade ahead is more likely than not.” 11 Allison has had a great deal of company in his alarming pronouncements. In 2007, the distinguished physicist Richard Garwin put the likelihood of a nuclear explosion on an American or European city by terrorist or other means at 20 percent per year, which would work out to 91 percent over the elevenyear period to 2018.12

Allison’s time is up, and so is Garwin’s. These oft-repeated warnings have proven to be empty. And it is important to point out that not only have terrorists failed to go nuclear, but as William Langewiesche, who has assessed the process in detail, put it in 2007, “The best information is that no one has gotten anywhere near this. I mean, if you look carefully and practically at this process, you see that it is an enormous undertaking full of risks for the would-be terrorists.” 13 That process requires trusting corrupted foreign collaborators and other criminals, obtaining and transporting highly guarded material, setting up a machine shop staffed with top scientists and technicians, and rolling the heavy, cumbersome, and untested finished product into position to be detonated by a skilled crew, all the while attracting no attention from outsiders.

Nor have terrorist groups been able to steal existing nuclear weapons—characteristically burdened with multiple safety devices and often stored in pieces at separate secure locales—from existing arsenals as was once much feared. And they certainly have not been able to cajole leaders in nuclear states to palm one off to them—though a war inflicting more death than Hiroshima and Nagasaki combined was launched against Iraq in 2003 in major part under the spell of fantasies about such a handover.14

More generally, the actual terrorist “adversaries” in the West scarcely deserve accolades for either dedication or prowess. It is true, of course, that sometimes even incompetents can get lucky, but such instances, however tragic, are rare. For the most part, terrorists in the United States are a confused, inadequate, incompetent, blundering, and gullible bunch, only occasionally able to get their act together. Most seem to be far better at frenetic and often self-deluded scheming than at actual execution. A summary assessment by RAND’s Brian Jenkins is apt: “their numbers remain small, their determination limp, and their competence poor.” 15 And much the same holds for Europe and the rest of the developed world.16 Also working against terrorist success in the West is the fact that almost all are amateurs: they have never before tried to do something like this. Unlike criminals they have not been able to develop street smarts.

Except perhaps for the use of vehicles to deliver mayhem (though this idea is by no means new in the history of terrorism), there has been remarkably little innovation in terrorist weaponry or methodology since 9/11.17 Like their predecessors, they have continued to rely on bombs (many of which fail to detonate or do much damage) and bullets.18

#### No motive, no opportunity

--CBRN = chemical, biological, radiological, nuclear weapons

Koblentz 20 Dr. Gregory D. Koblentz, Associate Professor and Director of the Biodefense Graduate Program at George Mason University's Schar School of Policy and Government; “Emerging Technologies and the Future of CBRN Terrorism;” The Washington Quarterly, Vol. 43, 06-16-2020, Issue 2, Accessed through T&F, <https://doi.org/10.1080/0163660X.2020.1770969> /GoGreen!

Cautions and Caveats

It is important to note that scientific advances and the emergence of new technologies are not the only, or even the most important, factors influencing the likelihood of terrorist groups acquiring and using CBRN weapons. Thankfully, the number of terrorist groups motivated to acquire these weapons has been limited, despite many that have the requisite technical and financial resources.60 The vast majority of terrorist groups have been satisfied with conventional weapons such as guns and bombs. The surprising rise of the Islamic State and their repeated use of chemical weapons in Iraq and Syria, however, serve as a reminder that it only takes one group with the intent and capability to acquire and use CBRN weapons to pose a threat to international security.61

In addition, the ability of a terrorist group to convert CBRN-related material into a weapon depends on intangible factors such as tacit knowledge (the unarticulated knowledge that can only be gained through hands-on, trial-and-error experience or mentorship), the ability of the group to create and share such knowledge, and its ability to assemble and successfully manage interdisciplinary teams.62 Terrorist groups, especially those facing pressure from law enforcement and intelligence agencies, have had difficulties recruiting, retaining, and effectively utilizing individuals with the right combination of scientific, technical, and organizational skills to develop effective CBRN weapons.

Developing a CBRN weapon capable of causing mass casualties is also a very complex process. A scientific breakthrough that makes developing or acquiring one component of a weapon easier might not have any impact on the other stages in the weaponization process. Thus, the impact of a single scientific breakthrough or a novel technology on the acquisition of a CBRN weapon should not be exaggerated. For example, synthetic biology might make it easier for a non-state actor to create a pathogen, but that technology does not help terrorists improve their ability to disseminate the pathogen on a large scale.63

Likewise, it is important to assess the specific contributions that a particular technology can make to a specific aspect of the CBRN threat in practice, not just in theory. In the case of 3D printing, this manufacturing technology is not appropriate for working with metals that are toxic or radioactive. While microreactors are well-suited to covertly producing small quantities of highly pure chemicals, they are not well-suited to the production of most chemical warfare agents and precursors due to excessive heat generated by their synthesis and by the production of solid byproducts that would clog the microfluidic channels at the heart of this technology.64

Finally, advances in science and technology represent not just threats, but also opportunities to make it harder for terrorist groups to acquire CBRN weapons. Unmanned aerial and ground vehicles can be used for border security, CBRN weapon detection, and bomb disposal. For example, the EU is sponsoring the development of unmanned aerial and ground vehicles to investigate CBRN crime scenes under the ROCSAFE project.65 Biometrics and radio frequency ID chips can be used to improve physical security measures and inventory control to prevent unauthorized access to CBRN materials. Advances in science and technology are also leading to improved sensors that can be used to detect the production, transportation, and use of CBRN weapons. The development of dedicated laboratories and new techniques to analyze CBRN materials has also contributed to impressive advances in nuclear, biological, and chemical forensics, which are crucial for attribution.66

### AT: AM&E I/L

#### The impact’s absurd – no part of SC relationships are truly wasted and trying to mini-max them is as likely to harm as help – BUT the difference is so marginal it can’t affect the balance of power anyway

Reynolds 21 Dr. Phil W. Reynolds, visiting scholar at the Center for Futures Studies at the University of Hawaii, “Building Partner Capacity Is Great Power Competition: The Future of 333 Funds,” Small Wars Journal, 2-6-2021, <https://smallwarsjournal.com/jrnl/art/building-partner-capacity-great-power-competition-future-333-funds> /GoGreen!

Can the U.S. Department of Defense do two things at once: Operate in the gray zone and excel in great power competition? Not according to Tommy Ross and Stephen Tankel who argue that security assistance “is focused on the wrong countries and being used to build the wrong capabilities.” Their idea is that competition with China and Russia - great power competition (GPC) - is the priority and all instruments of national power must be bent to that end, at the expense of all other needs. Ross and Tankel conclude that the “United States is no longer well-positioned to use security sector assistance to “compete with China and Russia — especially in ‘gray zone’ activities short of war.” Ross is a former assistant Secretary of Defense for Security Cooperation and should know better.

Changes in administrations are an opportunity to reflect on what works and what doesn’t, but in this case, changes in the name of so-called reform could cause real harm. They suggest, in part, converting what are known as building partner capacity (BPC) funds into general-purpose security assistance funds so they may explicitly be used for Great Power Competition — that is, to block China and Russia. That is a fine goal, but there are greater and more effective tools already in use. Security assistance writ large, about $19 billion dollars in 2019, and the deterrent effect of the U.S. armed forces being forward stationed and deployed around the world. Besides, Congress created specific categories of activities in for BPC which lie in the gray zone like counter terrorism operations, countering illicit drug trafficking, countering organized crime, supporting intelligence operations and supporting multi-national operations- like AMISOM in Somalia and the G5 Sahel. These funds are critical in providing equipment and training support against various insurgent, transnational terrorists and smuggling threats in twenty-one countries. Moving those funds from these conflicts to support great-power competition would result in the abandonment of those partners who are now decisively engaged on the United States’ behalf. There is real danger to a U.S. withdrawal of support to these fragile partners.

What are building partner capacity funds? They are a basket of congressional authorizations meant to counter urgent and emergent threats. In various forms, they have been around for three administrations. In the early 2000s, the DOD needed an authorization to quickly buttress and fund operations with smaller countries not in formal alliances like NATO or through the cumbersome existing security assistance framework of foreign military financing and sales. The zeitgeist of BPC funds was to quickly provide rifles, trucks, radios, and ammunition, along with training, to partner states who were fighting terrorists and insurgencies that were critical to U.S. security. These funds were meant for partner states actually engaged in the business of killing bad guys. Beyond Iraq and Afghanistan, which gobbled up billions of dollars, building partner capacity funds have been small. BPC funds have gone through several iterations since their introduction in 2006. The 2017 National Defense Authorization Act re-authorized the largest part of the funds under section 333. They have never exceeded 1 percent of the DOD budget. In 2020, 333 Global Train and Equip fund, made up less than 0.14% of the defense budget.

Where have 333 funds been used? Since 2017, they have been used in Burkina Faso, Chad, Cameroon, supporting Uganda, Kenya, and Djibouti in the UN mission in Somalia. Worldwide, they have been used in the Philippines, Vietnam, Jordan, Uzbekistan and even Mexico. Earlier versions of BPC funds were used in Hungary, Indonesia, Georgia, Latvia, Kazakhstan, Lebanon, Malaysia, the Philippines, Sri Lanka, Poland and Romania. In Africa in particular, the need is urgent. That is exactly where these funds should be deployed to allow the rest of the billions and billions of dollars of security assistance to be spent more directly against China and Russia in.

A Holding Action

First and foremost, building partner capacity is a holding action, a strategic defensive effort in order that the United States and its Allies can deter Russia and China with infantry divisions, fighter jets and aircraft carriers in other theaters. Building partner capacity (BPC) funds are not meant to be decisive. They buy time against the violence and instability of the gray zone. That zone is where malign actors create chaos and seek to replace legitimate authority in its wake. On one side is the area the U.S. and the international community can access, and on the other, are the forces that seek to confront the U.S. In Burkina Faso, Mali, and Niger, attacks by Islamic State and al Qaeda affiliates have increased dramatically since 2015, with more than 4000 deaths reported in 2019. The U.S. must stay engaged in that gray zone. This is the penultimate problem with the assertion that security assistance is out of sync with U.S. priorities and these “shortcomings hinder U.S. allies and partners, in turn leaving them vulnerable to Chinese and Russian influence” that reveals a deep misunderstanding of the strategy behind BPC funds. BPC funds are exactly how the U.S. remains engaged in competition with Russia and China in the gray zone.

A withdrawal of BPC funds or redirection in their uses would be tantamount to abandonment of the ideals of building up partners. The Department of Defense could just find itself in a deeper hole ten years hence, anxiously requesting another funding stream to counter the same, bigger, more dangerous threats. That is on the horizon: For example, Burkina Faso is the focal point of an increasingly complex regional war in which jihadist groups take advantage of nonexistent border security. This in turn has exacerbated and amplified local grievances about corruption and bad governance. An attack killed 36 in a village market in January 2020, and in October, another 20 were killed in the north of the country. The violence moves across international borders with impunity. This is typical of the vast trans-Sahel region in which the reach of the central state governments closely follows the roads and towns, with millions of square kilometers of scrub and desert left with only the lightest touch of government authority. In 2012, the National Movement for the Liberation of Azawad in Mali teamed up with heavily armed Toureg nomads back from the Libyan Civil war. The group captured key cities and declared northern Mali an Islamic state. The short, sharp civil war toppled the Malian president in a coup in March 2012, resulting in the French Government deploying 4,000 soldiers to push back the Islamist groups. In August 2020, another coup toppled the latest leader of Mali. Building partner capacity funds are used in each country for air reconnaissance assets, long range communications, and heavy-duty desert vehicles, along with training on how to tie them all together in operations. This contributes to partner’s internal stability, thus keeping them in the fold of international norms and values, and more resistant to Chinese and Russian influence.

China and Russia behind the Gray Zone

If the U.S. pulls back from these areas of conflict, China and Russia will step in. In many cases, it is because of the security situation and corruption that U.S. companies hesitate to operate. For China and Russia, concerns over human rights abuses matter little. Chinese investment in Africa tops $200 billion per year and since 2015, Beijing has provided $120 billion in financial aid. In Burkina Faso, China is building a $140 million hospital and a $1.3 billion dollar road. In Guinea, another west African country, China has provided $20 billion in loans to develop bauxite mines and another $14 billion for iron developments. In Mali, the Chinese have invested $11 billion in infrastructure deals.

It is true that many of these failing states are run by corrupt, narcissistic family and clan confederations whose human rights records are little better than the insurgent terrorists who seek to replace them. Security assistance funds provide an important foot in the door for the U.S. in these developing nations. It is particularly important because these weak countries view many of the U.S. State Department’s activities as subversive and possibly corrosive to their own authority. Building partner capacity (BPC) funds are security funds and that is simple enough to understand. If this ‘foot-in-the-door’ is removed, Chinese dollars will work just as well, their thinking goes. If the U.S. were to retreat along the line presented by Ross and Tankel, the line of instability would move, allowing the space behind to be filled by Russia and particularly, China. The places where Chinese money is invested would need security and already China has peacekeepers in Congo, Liberia, Mali, Sudan and South Sudan. China also partially funds the G5 Sahel Joint Force.

Perhaps more baldly, and thus more surprising that Ross and Tankel missed it, these small countries vote in the big international organizations, like the United Nations and the World Trade Organization. These potential allies will be needed in the coalitions of international cooperation that President Joe Biden looks to lead. Thwarting Russia and China short of actual war will require a broad coalition of countries voting on issues ranging from climate change to fair trade. Already, China uses dollar diplomacy to keep vulnerable, weak states in its orbit. It won over Burkina Faso in 2019, at the same time China offered to pay for security forces in the Sahel. BPC funds, for all their simplicity, can help buy votes, too.

The Last 1%?

Great power competition is real and is the priority of the Department of Defense. Ross and Tankel are correct in that. However, they lose sight of the billions and billions spent on great power competition. Since it is the priority, one could say that great-power competition consumes 99% of the Department of Defense budget. That is tanks, aircraft carriers, attack helicopters and missiles. That is personnel and their pay and benefits. That is all the training and exercises in the plains of central Europe and the seas in Southeast Asia. The U.S ability to curtail Chinese and Russian expansion in the gray zone is enormously important. Why would the last 1% be eyed for use in Europe and Northeast Asia?

It is because the bureaucracy simply cannot imagine low-level conflict as a useful means to a larger end. Slow to adapt, grinding, and loath to change, the Department of Defense was created for great power war and it requires expensive kit- missile defense, ships, tanks and fighter jets like the trillion dollar F35 and B21 programs, and the Gerald Ford aircraft carrier. Security assistance, run through the State Department, and the even bigger foreign military sales efforts have provided this kind of equipment since the 1960s. There is seduction in the simplicity of big wars. They are easy to understand, plan for, and win. From pre-commissioning training to the flag officer level, planning is oriented toward maneuvering divisions, corps and carrier air wings, the gotterdammerung of the decisive battle (a horrible misapplication of Clausewitz). This is the American way of war, with technology, mass, and speed. Unfortunately, this creates an amaranthine loop of organizational bias and coercive information processing routines that in turn produce values and norms about the way things are and the way things should be. BPC funds are meant for smaller, simpler tasks, not part of the U.S. main effort in its big wars. After 9/11 the Department of Defense needed a tool for engagement- thus the creation of these types of funds. Planning and execution have proceeded apace since. Ross and Tankel have also taken to task the planning superstructure for these funds. Their suggestion of creating “coordinated, department-wide planning processes at the departments of State and Defense” is also wide of the mark. There is already a joint review and approval process that begins eighteen to twenty-four months out from execution. There is even a capstone review conference called the Joint Security Sector Assistance Review that seeks to capture issues and recommendations for improvement in future execution cycles. Creating new human infrastructure, boards, bureaus, cells, and diagrams would invite more of the very “inefficient and incoherent planning and coordination processes” that Ross and Tankel seek to improve.

Considering the price point and investment level of BPC funds, they have been successful. They have paid for support to the AMISOM peacekeeping mission in Somalia and strengthened the Jordanian efforts against ISIS and Al Qaeda. They proved instrumental in providing real capabilities in Tunisia’s struggle against trans-national violence spilling over from Libya. The 333 funds, and other, even smaller building partner capacity authorizations have made a difference in these places where the average cost per capacity building program is just $5.5 million. There does exist the dubious idea is that these small funds could be deployed quickly to support and guide partners towards larger, and much more lucrative purchases of military equipment. This destroys the original intent of 333 funds. Congress has seen the importance of having separate authorities to do separate things, and this should be preserved. If BPC funds are amalgamated into the framework that provides big weapons and expensive capabilities, like fighter-jets, hyper-advanced, secure communications, and cyber security apparatus, it will take away, in some cases, the only incentive for partners to meet and fight terrorists. The knock-on effect is losing a strong method for deterring method of deterring Chinese and Russian aspirations in these gray zones.

Conclusion

Overall, the U.S. spends about $18 billion globally on various security assistance authorizations. The question that appears not to be asked in wise councils is "Would this tiny .14% make a difference in great power competition?" Already, the vast majority of security assistance funding does go towards great power competition via foreign military financing and sales. Other initiatives are not small. The European Deterrence Initiative focused on Russia sits at $6 billion, the Ukraine Security Assistance Initiative, provides $250 million, the Southeast Asia Maritime Security Initiative is funded at $425 million. Congress is set to authorize the Pacific Deterrence Initiative with has much as $6 billion over two years. Now, the bureaucracy wants the .14 percent of the budget meant to fight terrorism around the world.

Finally, the U.S. pays $700 billion a year for the world’s largest defense establishment on the premise that this massive juggernaut is needed for deterrence. In this case, it doesn’t make sense that another $700 million will make a difference. The very idea is staggering: Is there no deterrent effect in all those divisions and aircraft carriers? There is, however, a very real deterrent in strengthening small partners quickly and effectively. The Department of Defense can walk and chew gum at the same time. At least Congress thinks so, hence the categories legislated in the building partner capacity authorization. The U.S. will not send infantry divisions to west Africa; it can and should support governments in improving their own security. The DOD can confront China, Russia and provide capacity support to friends in the fight. For less than a billion dollars a year, the decision is a no-brainer.

#### Empirics disprove – AM&E itself is waste

Görgens 5 Marelize Görgens, World Bank, HIV/AIDS Monitoring and Evaluation consultant, “Monitoring and Evaluation Systems for HIV/AIDS: chasing data or challenging paradigms?” November 2005, <https://www.researchgate.net/publication/291347597_Monitoring_and_Evaluation_Systems_for_HIVAIDS_chasing_data_or_challenging_paradigms> /GoGreen!

Within the international development arena, the past few years has witnessed a move towards measured, progress-focused development, as illustrated by the birth of terms such as “effective aid ” and “managing for development results ” at various international forums. For example, at a global meeting of development partners in 2004, , the discussions centred on how to strengthen an international partnership around the concept of ’managing for development results’. This upped the stakes for monitoring and evaluation (M&E), in the sense that the Joint Memorandum, which was issued by all these global partners at the end of their meeting, focused not only on M&E processes itself, but also on using results for improvement and decision-making.

“[We will] rely on – and strengthen – countries’ monitoring and evaluation systems to track progress and assess outcomes. As agencies with regional or global reach, we pledge to better distill the lessons of countries’ experiences and disseminate knowledge about what gets results in different country contexts.”

Joint Memorandum, issued by all global development partners at the end of the 2nd Roundtable on Managing for Development Results

Despite pressure from international development partners to measure and quantify results, M&E has remained the ugly duckling of development. Efforts to incorporate it into practice have met with a combination of apathy, resistance, and half-baked efforts that primarily consisted of throwing together a few indicators and defining how the data would be collected.

Developments in the field of HIV/AIDS monitoring and evaluation over the last 10 years has illustrated the challenges of monitoring and evaluating of development efforts in general, and raised some uncomfortable, close-to-home questions for the development M&E profession.

In Africa in particular, HIV/AIDS M&E is not only important because of international pressure on managing for development results, but also because of the scale of the virus’s impact. HIV/AIDS has ravaged Africa. A continent-wide Social Impact Assessment would have revealed that it has destroyed families, torn apart communities, paralysed the health sector, crippled the agricultural and education sectors, hampered government’s efforts to provide effective services to its people, and caused indescribable long-term trauma and grief. The extent and reach of its impact over such a short period of time is forcing national AIDS coordinating structures to focus, maybe for the first time, on ways to find real, effective, efficient, and replicable solutions.

At the international level and at the country level, the response to HIV/AIDS has moved in the past 10 years from a health sector-driven to a multisectoral response. In parallel, HIV/AIDS monitoring and evaluation has evolved from exclusively epidemiological surveillance in the 1980s to multi discipline approaches to HIV/AIDS M&E.

B What are the challenges?

HIV/AIDS M&E cannot be a disjointed collection of evaluation studies and monitoring processes, but needs one integrated HIV/AIDS M&E system, managed by a National AIDS Commission (NAC) MG comment: some countries do not have NACs, so it may be better to refer to it as the national AIDS coordinating structures. This is because the NAC has the mandate to coordinate and manage the national HIV response and can only do this if it has accurate and relevant data when decisions need to be made. It is also because it was recently acknowledged, internationally, that one M&E framework at country level is one of the core principles of effective management of the HIV response .

Such an HIV/AIDS M&E system needs to combine a vast variety of M&E processes: from biological sentinel surveillance (an epidemiological “tripwire” used to detect trends in HIV infection); to routine collection of management information about funding for HIV interventions in the public sector, private sector and civil society; and ethnographic-type studies about sexual risk behaviour and the abuse of right of vulnerable children, the elderly and persons living with AIDS.

HIV/AIDS M&E requires that, in order to assess the extent and nature of HIV service coverage, the same output-level, programme-monitoring data be collected from all implementers of HIV interventions on a routine basis. The health sector in Africa has struggled to establish an effective management information system in its own sector – NACs are now obliged to set up a such a routine system across all government ministries, the private sector, and the entire civil society. This is a vast undertaking, especially given that some of these organisations have never had to report to government before. Another challenge is that the HIV response is increasingly becoming decentralised. This adds a layer of reporting and could potentially cause delays in data collection.

HIV interventions range dramatically in content, focus, and implementation methodology. For example, interventions focusing on establishing partnerships for HIV will have vastly different monitoring and evaluation approaches to programmes that aim to keep educationally marginalised children in school.

The impact of HIV has necessitated that there is a real focus on using results for decision-making and programme improvement because countries in Africa heavily burdened by HIV/AIDS cannot afford not to.

B What can be done?

Addressing these challenges requires a systemic approach: we need to focus on designing and operationalising national HIV/AIDS M&E systems, rather than new evaluation studies.

Figure 1 illustrates such a systemic approach to HIV/AIDS M&E. It shows the relationship between indicators (A), data sources (B), information products (C) and the project stakeholders (D). These four components will only work in unison if it is backed up by strong management.

Figure 1: Illustration of Systemic Approach to HIV/AIDS M&E

At the risk of revamping an old development phrase, a systemic approach to HIV/AIDS M&E require those involved in the M&E profession to change. It requires a paradigm shift away from conducting piecemeal, complicated, and specialised monitoring or evaluation studies and towards thinking about monitoring and evaluation in an operational way, focusing on synergies, sometimes at the expense of individual academic accolades.

B The Way Forward

Such an approach requires that M&E professionals:

•Learn new skills: they need to become good budgeters, M&E work plan developers and M&E strategists.

•Move away from focusing on specific processes and towards integrated monitoring and evaluation systems, which re-examines the practicalities of collecting output data.

•Use existing tools in a new way: For example, Social Impact Assessments have, to date, primarily been used to assess the impact of planned developments (e.g. assessing the social impact of a new mine on a community’s livelihood). The tools in the quiver of the Social Impact Assessment process (including trend extensions, computer modelling, consulting experts, focus group discussion and questionnaires) could be adapted to even suit assessments of the unplanned, catalytic, and widespread impact of HIV and AIDS on different sectors of society.

•Assess the cost-benefit trade-off in different monitoring and evaluation tools and processes to find, recommend, and use those processes that are most useful for the most reasonable cost

•Be prepared to sacrifice some professional autonomy for the sake of synchronisation. In one country in Africa, in 2004, over 40 assessments relating to HIV/AIDS M&E were done, often replicating each other.

•Understand how HIV/AIDS M&E systems should be managed to yield the best possible success; it implies advocacy for M&E, capacity building in M&E and communications about M&E

•Find a renewed focus to make sure that results are used to improve projects.

•Go back to the basics of data collection, and apply it with new vigour in a multi-sectoral, decentralised, developing and emergency context.

•Think of practical ways in which to focus on, promote and institutionalise the process of using results for decision-making. This means moving away from the typical thinking in which M&E systems have focused on indicators and data sources, with less focus on information products and dissemination to stakeholders (see Figure 2). It also implies avoiding a situation where stakeholder dissemination is done as an afterthought, primarily through a national level workshop.

Figure 2: Disproportionate focus on Indicators and Data Sources

The challenges of HIV/AIDS monitoring and evaluation systems cut to the heart of the monitoring and evaluation profession. Although we have always known that monitoring and evaluation needs to earn its keep (Patton, 2000), it is nowhere more evident than in the design and implementation of HIV/AIDS M&E systems. Every dollar that is spent on monitoring and evaluation is one that it not spent on HIV programme implementation. Within the context of HIV/AIDS, this can simply not be wasted.

HIVAIDS is an opportunity for our profession to prove M&E as a real, tangible and value adding part of development work, and as an opportunity for professionals to demystify monitoring and evaluation. We have a responsibility to do so, and there has never been a better time.

#### Even if it works, results won’t be used effectively

Lahaye 20 Estelle Lahaye, Senior Financial Sector Specialist at CGAP, former account manager in Luxembourg at Banco Itaú Europa, MS Business, San Francisco State University, BS banking, finance, and insurance, University of Nancy 2 in France; and Alice Nègre, Senior Financial Sector Specialist at CGAP, graduated from ESCP, Paris; “How Can Funders Avoid Chasing Data as the Latest Shiny Object?” CGAP Blog, 12-8-2020, <https://www.cgap.org/blog/how-can-funders-avoid-chasing-data-latest-shiny-object> /GoGreen!

We don’t need to preach to the choir: given the plethora of data-related projects that donors and development finance institutions (DFIs) have supported in the past, they clearly know that data is a powerful tool for advancing financial inclusion. And there is a lot to be excited about, given how digital technologies are accelerating the speed, depth and breadth of available data.

We share this excitement. In fact, data is at the heart of CGAP’s work. In recent years, we have talked about data-based segmentation to better serve customers, data sharing to enable innovation, data protection and how data capabilities need to be revamped to implement risk-based supervision.

But is data just the latest shiny object of the financial inclusion community? Are data’s powers fully leveraged? Does more data lead to sustainable impact?

Today, we think the jury is out on all three of these questions. Our research shows that more and better data in the hands of providers, regulators, policy makers, investors and customers doesn’t automatically lead to better outcomes. Results often show that these market actors do not use data or have stopped using data after a while.

That’s why, for us, the real excitement lies beyond data. It is about bringing fresh thinking to help donors and DFIs achieve sustainable impact through their data efforts. Based on our research, we have four recommendations:

Do not overestimate data as a driver of change. Increased knowledge with data does not necessarily incentivize behavior change. For example, robust data on women's demand and need for financial services will not automatically lead providers to improve their suite of products and services. A detailed theory of change (ToC) will help donors and DFIs to clarify the chain of incentives and behavior changes that a data initiative seeks to trigger. Make sure the pathway from data to expected outcomes is clear.

### Thumper – Ukraine

#### Ukraine thumps – and more unexpected arms increases are coming

Ryan 6-14-22 Missy Ryan, reports on diplomacy, national security and the State Department for The Washington Post; and Emily Rauhala, Brussels bureau chief for The Washington Post, covering the European Union and NATO; “Ukraine battle intensifies as Western backers mull new military aid,” The Washington Post, 6-14-2022, <https://www.washingtonpost.com/national-security/2022/06/14/severodonetsk-weapons-nato-russian-advance/> /GoGreen!

Russia intensified its assault on a strategic Ukrainian city on Tuesday as NATO officials prepared to debate increased military support for Kyiv’s attempt to reverse Russian momentum in the country’s east.

Officials in the eastern city of Severodonetsk said that Ukrainian forces were mounting a pitched defense of an area that is now a central focus of Russian firepower. Mayor Oleksandr Stryuk described “constant fighting” for Severodonetsk, which has become increasingly isolated following the destruction of bridges leading out of the city. He said Russian troops so far have been unable to complete their control of the area.

“Street fighting is underway,” Stryuk said. “Tactically, our armed forces are pushing back the enemy,” an effort that he said relies on a “huge amount of manpower.”

Serhiy Haidai, governor of the Luhansk region where Severodonetsk is located, said that humanitarian supplies could no longer be delivered to the city. The two sides have exchanged accusations about who is responsible for destroying the bridges, which permit the movement of civilians and aid but also military equipment and troops.

Capturing Severodonetsk and neighboring Lysychansk, which lies across the Siversky Donets river, would represent a major step forward in President Vladimir Putin’s quest to solidify control of eastern Ukraine, and would mark a Russian revival following the battlefield failures that characterized the early stage of the war.

Even as Ukrainian forces face mounting setbacks in the Donbas campaign, officials in Kyiv have vowed to retake every inch of Russian-controlled territory, including Crimea, which Russia annexed in 2014, but they say greater outside help is required.

Haidai said conditions for civilians remaining in Severodonesk are now “extremely difficult.” In echoes of the extended siege of the southern city of Mariupol, officials have said that some 500 people, including dozens of children, are sheltering in bunkers beneath the city’s Azot chemical plant.

On Tuesday, a top Russian military official offered a humanitarian corridor to permit the evacuation of civilians trapped at the plant. In a statement, Col. Gen. Mikhail Mizintsev said the evacuees would be permitted to travel to the Russian-controlled city of Svatove. Ukrainian civilians forced to evacuate to areas under Russian control have complained of abuse and degrading treatment at filtration camps.

Mizintsev, who heads Russia’s National Defense Control Center, accused Ukraine of positioning civilians at the plant as human shields. He demanded the surrender of Ukrainian troops there, characterizing them as “militants of nationalist battalions and foreign mercenaries.”

Ukrainian President Volodymyr Zelensky renewed his appeal on Tuesday for greater military aid to help Ukraine defend itself in Luhansk and other areas, saying that only greater quantities of air and missile defense systems can help stave off Russia’s larger, more advanced military. Those weapons are expected to be of increased importance in the artillery-heavy battle for the Donbas region.

Zelensky cited missile attacks near Lviv and Ternopil on Tuesday, which he said Ukrainian forces had been able to only partially defend against.

“We keep telling our partners that Ukraine needs modern antimissile weapons. Our country does not have it at a sufficient level yet,” he said in a nightly video address. “Delay with its provision cannot be justified.”

How much new weaponry is provided, and what kind, may be defined on Wednesday when officials gather in Brussels for a meeting of the s Ukraine “defense contact group,” which will be chaired by U.S. Defense Secretary Lloyd Austin.

Austin touched down in Belgium on Tuesday ahead of that gathering, which is expected to include up to 50 countries, and a separate meeting of NATO defense ministers being held ahead of a June 29 alliance summit in Madrid.

When NATO foreign ministers convened in April, Ukraine told the alliance its priority issue was “weapons, weapons, weapons” — a message that is likely to be reiterated this week as the conflict drags through its fourth month.

While the Biden administration has not revealed its plans, the Pentagon’s top policy official on Tuesday suggested it would send additional multiple-launch rocket systems to Ukraine, potentially going farther to satisfy Ukrainian demands.

Colin Kahl, who serves as undersecretary of defense for policy, said the four M142 High Mobility Artillery Rocket Systems, which can hit targets at longer distance, that Washington has sent to Ukraine to date did not represent the end of its supply of such weapons.

“We’re going to provide the Ukrainians what they need to prosecute the targets inside Ukrainian territory,” Kahl said during a think tank event in Washington. Ukrainian officials have said they need at least 60 such systems.

Western leaders have gradually increased the array of arms they are willing to provide Ukraine since the beginning of the war. But many remain nervous about supplying systems that could be used to launch attacks deep into Russian territory or that Putin might use as a reason to strike a NATO country.

In separate discussions in Brussels on Thursday, NATO allies are expected to discuss a range of broader issues, including the alliance’s troop footprint in Eastern Europe and defense spending, conversations that will continue at the late June summit in Madrid.

#### Ukraine will remain a more urgent priority

DoS 6-1-22 U.S. Department of State, Bureau of Political-Military Affairs, “U.S. Security Cooperation with Ukraine,” Fact Sheet, 6-1-2022, <https://www.state.gov/u-s-security-cooperation-with-ukraine/> /GoGreen!

The United States, our allies, and our partners worldwide are united in support of Ukraine in response to Russia’s premeditated, unprovoked, and unjustified war against Ukraine. We have not forgotten Russia’s earlier aggression in eastern Ukraine and occupation following its unlawful seizure of Crimea in 2014. The United States reaffirms its unwavering support for Ukraine’s sovereignty and territorial integrity within its internationally recognized borders, extending to its territorial waters.

Ukraine is a key regional strategic partner that has undertaken significant efforts to modernize its military and increase its interoperability with NATO. It remains an urgent security assistance priority to provide Ukraine the equipment it needs to defend itself against Russia’s war against Ukraine.

Since January 2021, the United States has invested more than $5.3 billion in security assistance to demonstrate our enduring and steadfast commitment to Ukraine’s sovereignty and territorial integrity. This includes more than $4.6 billion since Russia’s launched its premeditated, unprovoked, and brutal war against Ukraine on February 24. Since 2014, the United States has provided more than $7.3 billion in security assistance for training and equipment to help Ukraine preserve its territorial integrity, secure its borders, and improve interoperability with NATO.

### Thumper – Taiwan

#### Taiwan thumps – it’s being prioritized

Nakamura 6-13-22 Ryo Nakamura, Nikkei staff writer, “U.S., Taiwan set to hold strategic dialogue this month: sources,” Nikkei Asia, 6-13-2022, <https://asia.nikkei.com/Politics/International-relations/U.S.-Taiwan-set-to-hold-strategic-dialogue-this-month-sources> /GoGreen!

The U.S. and Taiwan are in the final stages of preparation for a strategic bilateral dialogue between security officials, three people with knowledge of the matter told Nikkei.

The dialogue, scheduled to take place by the end of this month in the U.S., is expected to focus on specific measures for weapons provision and military drills.

Officials from the two sides will discuss details of security cooperation under a regular framework known as the "Monterey talks" -- last held in autumn 2021 in the U.S., according to Taiwanese media. As a general rule, neither plans for the talks nor details are publicly disclosed.

One of the sources said the key theme for the upcoming dialogue would be weapons support from the U.S., with Washington aiming to prioritize the sale of weapons that would be effective in blocking potential Chinese landing operations on the island.

The U.S. Congress is considering a plan to provide several billion dollars of financial support to Taiwan so the island can procure weapons, Nikkei reported last month, citing three sources connected to the legislature.

The Biden administration intends to prioritize the sale of weapons with what it calls "asymmetric capabilities" -- those that are agile, inexpensive and effective in dealing with Chinese amphibious operations. Specifically, they cover anti-ship missiles and air defense systems, as well as systems for gathering intelligence needed to identify enemy movements and for initiating early warnings.

But F-16 fighter jets, which the U.S. government has already decided to sell to Taiwan, might not fall under this category. This implies that the bar for additional fighter jet sales may be set higher in the future.

By prioritizing asymmetric weapons, the U.S. intends to quicken reinforcement of capabilities in preventing the Chinese military from landing operations on Taiwan. It also aims to encourage Taiwan to allocate its budget more efficiently on the defense front.

It appears that the U.S. has prepared a list of weapons and systems it recommends Taiwan to purchase, and selected about 20 specific weapons and other items as preferred subjects of sale.

Taiwan was a hot theme at the weekend's Shangri-La Dialogue security summit in Singapore.

"Now, as a part of our One China policy, we will continue to fulfill our commitments under the Taiwan Relations Act," U.S. Defense Secretary Lloyd Austin said on Saturday. "And that includes assisting Taiwan in maintaining a sufficient self-defense capability."

### N/L – No Tradeoff + Thumpers

#### NO link uniqueness NOR internal link – there will always be a higher-priority SC crisis – Ukraine and Taiwan thump – AND black swans are inevitable – BUT DoD planners can walk and chew gum

Sprenger 22 Sebastian Sprenger, Europe editor and former managing editor for Defense News; Joe Gould, senior Pentagon reporter for Defense News; “US military readies to ‘walk and chew gum’ as multiple crises loom,” Defense News, 1-28-2022, <https://www.defensenews.com/global/europe/2022/01/28/us-military-readies-to-walk-and-chew-gum-as-multiple-crises-loom/> /GoGreen!

As roughly 100,000 Russian troops amass around Ukraine, a series of emerging crises around the world — the Middle East, China, North Korea — are demanding the full attention of NATO, and particularly its most powerful member, the United States.

Now, there’s a growing sense among national security experts that the crisis in Ukraine is just one of many conflicts on the precipice, putting pressure on the alliance and its member countries to address this threat and at the same time brace for the next one.

Indeed, China this week flew 39 warplanes toward Taiwan. And consider the United Arab Emirates reported this week it had intercepted multiple ballistic missiles aimed at Abu Dhabi.

Julianne Smith, the U.S. ambassador to NATO, described the ongoing dispute between Russia and Ukraine as a “microcosm” of the types of threats Western analysts were expecting all along. “All of this is becoming very real,” she said this week at a panel in Brussels sponsored by the German Marshall Fund of the United States.

At the same time, “something could happen on China and Taiwan next week,” said Ian Lesser, vice president at the think tank, referring to the possibility of China attacking the U.S.-backed island nation that Beijing sees as a renegade province to be eventually united with the mainland.

Asked about that possibility on Thursday, Defense Department spokesman John Kirby said the military remains watchful of other theaters.

“I think the gist of your question is, why can’t we walk and chew gum at the same time,” he told reporters at the Pentagon. “We can, and we are. … Just because we’re focused on bolstering our allies because of the worrisome accumulation of combat-credible power by the Russians in and around Ukraine doesn’t mean that we aren’t focused on the pacing challenge that China represents to the department.”

As NATO tries to use diplomacy to defuse tensions in Ukraine, planners are finding the standoff reflects many of the characteristics slated to make up the alliance’s new strategic concept.

Analysts have long said the upcoming revision, up for approval at the alliance’s Madrid summit in late June, must consider defenses against information warfare, cyber attacks, economic pressure and an overall increase in conflict complexity that exceeds that of traditional military operations.

Much of that is happening right now,

With NATO and U.S. written responses delivered to Moscow on Wednesday, diplomacy is still running its course. Russia wants the alliance to close the door to an eventual Ukrainian membership, a prospect considered notional at best even within NATO.

Alliance officials, in turn, have touted the principle that Russia’s neighbor nations should be able to pick their own path in matters of defense and security.

That idea doesn’t sit well with the Kremlin, where President Vladimir Putin is nursing dreams of restoring past Russian grandeur along ethnic, religious and language lines, incorporating some of its neighbors, according to Western analysts.

Still, the guns remained silent on mid-day Friday.

“I think the West is doing fairly well in managing a conflict that cannot be deterred,” said Hal Brands, a senior fellow with Washington-based American Enterprise Institute, a conservative think tank, and a professor at Johns Hopkins School of Advanced International Studies.

Brands said he believes Moscow’s demands were so outrageous an eventual armed confrontation was likely baked into them from the start. At this point, he said, Putin may be more interested in continuing the pace of escalation rather than agreeing to a diplomatic solution.

Deterrence has been the name of the game in Europe, however, where countries are trumpeting weapon shipments large and small into Ukraine, publicly scorning the one government not going along: Berlin.

European countries still view their relationship with Russia through bilateral lenses, said Rachel Rizzo, an analyst with the Atlantic Council think tank. “That’s why they are sidelined,” she added, referring to the fact that the European Union has no formal role in the ongoing negotiations.

German government officials have defended their position of sending only help that neither shoots nor explodes, like helmets, arguing a plus-up in combat capabilities would be too insignificant to warrant undermining Berlin’s policy of hopeful hedging. But inside the country, some analysts are arguing it’s time to take a stance militarily.

The situation is emblematic for how disjointed Europe’s position continues to be on key defense issues, and how its biggest economic player is finding itself isolated, said Christian Mölling of the Berlin-based German Council on Foreign Relations.

“We have left a vacuum that the Americans are forced to fill once again,” he said.

### N/L – No Tradeoff XT

#### There’s no trade-off between AM&E and SC programs

Shea 5 Colonel Timothy C. Shea, US Army, associate director of the Senior Executive Seminar for the College of International and Security Studies at the George C. Marshall European Center for Security Studies, “Transforming Military Diplomacy,” Joint Forces Quarterly, iss.38, 2005, <https://apps.dtic.mil/sti/pdfs/ADA522974.pdf> /GoGreen! \*added [eclipse]

The defense attaché system structure, mission, and manning have not evolved with the changes of the last decade that require increased levels of involvement in operational activity. The primary attaché function of observing and reporting is often considered to be in direct conflict with time and energy spent on other nonintelligence activities. Intelligence and military-diplomatic activity are not zero-sum competing requirements. Narrow specialization by other DOD elements has undermined the overall effectiveness of the military attaché by reducing access to the host nation military. DOD representation abroad should be the military attaché. Security assistance and arms control would be better managed by trained attachés with the requisite language skills, cultural knowledge, and regional expertise. This approach would eliminate parochialism, reduce overhead, streamline operations, and simplify bilateral coordination for the host nation military.

Transformation of the military attaché corps begins at the higher headquarters. The nature and function of a headquarters influence the priorities of its subordinate elements. By eliminating stovepipe organizations inside the U.S. Embassy in a consolidated DAO, the combatant command headquarters will need to establish a Politico-Military Directorate to manage, deconflict, and synchronize the activities of military attachés. This transformed organization will integrate national requirements for observing and reporting, supporting operational and exercise taskings, security assistance, and strategy and policy. More coherent policy and guidance will enable the military attachés to apply the informational instrument of national power more effectively. Making the director of this new organization within each combatant command a general/flag officer with attaché experience will brighten the promotion prospects for attaché duty and attract higher quality officers.

Realigned Mission Priorities

Security cooperation and the war on terror have increased the strategic importance of military attachés serving abroad. Considering the extensive actions to coordinate the deployment of U.S. forces against the Taliban in Afghanistan and support the train-and-equip operation in Georgia, attachés provide a tremendous value to the combatant commanders as operators and reporters. Independent of transformation, they have four main missions that seamlessly blend.

Advising the Ambassador. Military attachés must know the host nation military and strategic environment and be intimate with the U.S. military’s capabilities to support diplomatic and engagement measures. The DATT provides advice on the full range of issues concerning regional security, to include the attitudes and intentions of the host nation and other nations engaged in regional activities. Finally, most DATTs also serve as the U.S. defense representative charged with managing the coordination of administrative and security matters of all DOD personnel who fall under responsibility of the U.S. Ambassador. However, this command relationship would be more effective with defense attachés assigned to the same higher headquarters as the other DOD elements—the combatant command.

Representing DOD to the host nation. More than playing a ceremonial role, military attachés are a highly visible symbol of the Armed Forces. Especially critical in Eurasia where the Iron Curtain allowed for little interaction with Americans during the Cold War, they provide daily access to the host nation military regarding information, capabilities, and strategies. They are generally contacted before all others in a crisis. They serve a large public diplomacy function as well.

Reporting conditions in the host country. Attachés observe military conditions and developments. This is a continuous mission that must be integrated into all their activities. To succeed in security cooperation, policymakers and decisionmakers require actionable information. It is often attaché input that makes for effective security cooperation programs. During periods of heightened tension and crisis, the attaché supports the combatant commander by becoming his eyes and ears on the scene, responding quickly to time-sensitive information requirements. Increasingly, military attachés serve as the conduit for sharing information, especially in support of the war on terror. Lastly, corruption remains a huge problem in Eurasia, and military attachés provide oversight to monitor whether U.S. resources and funds are used appropriately.

Managing security cooperation programs. Worldwide, about half of all DAOs manage formal security assistance programs such as the International Military Education and Training (IMET) program and Foreign Military Financing (FMF). In activities unique to the former Soviet Union, the military attaché already plays a substantial role in coordinating and executing the extensive military-to-military programs, exercises, and deployments, which frequently dwarf [eclipse] IMET and FMF responsibilities. Even in countries with security assistance offices, attachés still make recommendations on spending priorities and approve IMET candidates.

Improved Manning Posture

Many DATT positions in remote regions are occupied by hard-working but junior majors or senior first-time attachés with limited choices for their terminal assignment. Lack of experience, language skills, rank, or maturity is not a recipe for success. Many countries recognize the strategic importance of their military attachés and send only their best abroad. Because of the symbolic and ceremonial importance of rank, and the requirement for experience and maturity, DATT billets should be filled by colonels (or Navy captains) and represented by the service that logically corresponds to that which dominates in the host country. Most importantly, DAOs must have sufficient depth to permit attachés to operate in multiple geographical locations.

To what degree is the United States able to resort to military power without dependence on foreign governments? The military attaché manages the day-to-day bilateral relations for national policymakers and combatant commanders. Transforming the attaché corps will substantially improve the steady state military diplomacy that must be conducted prior to any crisis. Changing the status quo will improve interagency coordination and provide the combatant commander the representation he needs within his area of responsibility. The military attaché corps must adapt to the new strategic environment, which demands skillful military diplomacy and knowledgeable professionals. Like the Special Operations Soldiers who achieved fame in Afghanistan by demonstrating their strategic value, military attachés have the potential to provide significant returns in the area of military diplomacy, while at the same time providing better reporting on a wider range of important issues.

### N/L – Budget Space

#### DoD’s programming is flexible – has the budgetary space to accommodate the plan

Bergmann 21 Max Bergmann, senior fellow at the Center for American Progress, focuses on European security and U.S.-Russia policy, formerly served in the U.S. Department of State as senior adviser to the assistant secretary of state for political-military affairs and special assistant to the undersecretary for arms control and international security, MA comparative politics, London School of Economics; and Alexandra Schmitt, senior policy analyst on the National Security and International Policy team at the Center for American Progress, MPP Harvard Kennedy School; “A Plan To Reform U.S. Security Assistance,” Center For American Progress, 3-9-2021, <https://www.americanprogress.org/article/plan-reform-u-s-security-assistance/> /GoGreen!

DOD officials can work around the State Department’s diplomats. In part due to restrictions from the Budget Control Act and with new programs at the DOD, Pentagon officials had more flexibility on security assistance programs than their State Department counterparts. The DOD had budgetary space to reallocate significant funds from the substantial Pentagon budget to respond to sudden emergencies or new crises, something that is virtually impossible for the State Department, making the DOD often the lead actor in a crisis.44 Regional combatant commands aggressively sought more resources from Congress to conduct their own security assistance programs, giving them added flexibility to work with partners in the field that their State Department counterparts lacked.45 A Government Accountability Office report found that 56 DOD security assistance programs do not require any involvement from the State Department.46

### N/L – Plan Funds

#### Funding is normal means

DoD 21 (Defense Security Cooperation University, Defense Security Cooperation Agency, U.S. Department of Defense, “Chapter 1 Introduction to Security Cooperation,” Security Cooperation Management (aka DSCU Green Book), Edition 41.0, May 2021, <https://www.dscu.edu/documents/publications/greenbook/01_Chapter.pdf>)

Train and Equip/Security Cooperation: Title 10 Programs

Under the authority of Title 10, Chapter 16, and/or the current National Defense Authorization Act, DoD provides material assistance and related training to partner nations to develop specific capabilities and/or capacities. This is normally done using DoD Operations and Maintenance (O&M) funding, but, in some instances, Congress appropriates additional funding for DoD to conduct these programs. Although it is DoD funding, these programs, and all security cooperation, must be coordinated with DoS. Security Cooperation practitioners refer to these programs as Building Partner Capacity (BPC) programs and execute them using a pseudo Letter of Offer and Acceptance. All BPC programs require congressional notification. Below are just a few examples. Examples with four digits in quotes represent temporary authorities whose authorizations can be found in various National Defense Authorizations Acts.

• “1022” Authority to Provide Counterdrug (CD)-Funded Support to Law Enforcement Agencies

• “1206” Training of Security Forces and Associated Security Ministries of Foreign Countries to Promote Respect for the Rule of Law and Human Rights

• “1226” Support to Certain Governments for Border Security Operations

• 333, Foreign Security Forces: Authority to Build Capacity

• Afghanistan Security Forces Fund (ASFF)

• European Deterrence Initiative (EDI)

• Iraq Security Forces Fund (ISFF)

• Counter ISIS Train and Equip Fund (CTEF)

• Indo-Pacific Maritime Security Initiative (MSI)

### N/L – Plan Cheap

#### Plan is cheap

Kelly 10 Terrence K. Kelly, principal mathematician at the RAND Corporation, former director of the RAND Homeland Security Research Division, formerly served for 20 years as a commissioned officer in the U.S. Army, positions included senior national security officer in the White House Office of Science and Technology Policy, PhD mathematics, Rensselaer Polytechnic Institute; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; Cathryn Quantic Thurston, Political Scientist at RAND, PhD Conflict Analysis and Resolution, George Mason University; Jennifer D. P. Moroney, senior political scientist at RAND, PhD international relations, University of Kent at Canterbury; and Charlotte Lynch, researcher at RAND; “Security Cooperation Organizations in the Country Team Options for Success,” RAND Corporation, 2010, <https://apps.dtic.mil/sti/pdfs/ADA517323.pdf> /GoGreen!

The U.S. military must plan for a wide range of security cooperation1 missions, ranging from “normal” peacetime security cooperation activities—such as building the long-term institutional and operational capabilities and capacity of key partners and allies, establishing and deepening relationships between the U.S. and partner militaries, and securing access to critical areas overseas—to managing quasi-operational efforts, such as managing foreign internal defense within the overall foreign policy objectives of the United States. Security cooperation, in the form of noncombat military-to-military activities, is a useful part of the military’s toolkit in conflict prevention.2 Although security cooperation requires a relatively small investment with respect to the overall efforts of the U.S. military, it can be a key enabler of the success of future U.S. military missions by shaping the environment and laying the groundwork for future coalition and stability operations with allies and partners.3

### N/L – Compartmentalized

#### AM&E is compartmentalized

Walther-Puri 21 Andrea Walther-Puri, PhD candidate, Fletcher School of Law and Diplomacy, research focuses on the effects of U.S. military counterterrorism programs on longer-term security governance transformation in the Sahel, “Afghanistan: A Tragic Lesson of the US Military’s Flawed Approach to Capacity Building,” Just Security, 9-6-2021, <https://www.justsecurity.org/78086/afghanistan-a-tragic-lesson-of-the-us-militarys-flawed-approach-to-capacity-building/> /GoGreen!

The FY2017 NDAA also included a crucial development: the creation of an in-house AM&E workforce at DOD. The Defense Security Cooperation University was founded in September 2019, to uphold a common knowledge base across the workforce, mandate common professional standards through a required multi-tier certificate program, and prioritize continued intellectual development. To further bolster this in-house AM&E workforce and minimize dependence on third-party contractors, the NDAA mandated the establishment of teams dedicated to AM&E within the Office of the Deputy Assistant Secretary of Defense for Security Cooperation, the Defense Security Cooperation Agency, and within each Geographic Combatant Command.

### N/U – Deprioritized

#### AM&E is already deprioritized

Cole 21 Emily Cole, program officer for governance, justice and security in the Applied Conflict Transformation Center at the U.S. Institute of Peace, MALD Fletcher School at Tufts University, BA Amherst College; and Dr. Calin Trenkov-Wermuth, security governance advisor at USIP, formerly worked at the U.N. Office of Counter-Terrorism, served in the NATO Parliamentary Assembly, PhD, MA international relations, University of Cambridge, BA world politics Hamilton College; “To Consolidate Democracy, Change U.S. Security Assistance,” U.S. Institute of Peace, 12-16-2021, <https://www.usip.org/publications/2021/12/consolidate-democracy-change-us-security-assistance> /GoGreen!

2. Enforce assessment, monitoring and evaluation requirements. The 2017 National Defense Authorization Act required better assessment, monitoring and evaluation of security sector assistance. U.S. government officials admit that this is not happening yet, and big strides need to be taken to implement and learn from security assistance monitoring and evaluation. This is one way to ensure programming is effective and that it helps broader strategic objectives, including the consolidation of democracy.

### U O/W – Requirements

#### AM&E is structurally inevitable – legally required! – and stuff’s been optimized

Maginnis 21 Robert Maginnis, contractor with Sigmatech Inc. supporting DASA (DE&C) as a global strategist, retired U.S. Army officer who recently completed 18 years with HQDA G-3/5/7 working security cooperation policy and training, MS management science, Naval Postgraduate School, BS engineering, United States Military Academy at West Point, graduate of numerous Army schools including the Command and General Staff College and the Army War College’s Strategy Course; and Michael Prater, principal adviser to the DASA (DE&C) for global security assistance and armaments cooperation, BBA acquisition and contracts management, Strayer University; “Security Cooperation Refresh,” Army AL&T Magazine, 9-2-2021, <https://asc.army.mil/web/news-security-cooperation-refresh/> /GoGreen!

Fortunately, those too often disjointed outcomes are now collapsing into a far more synergistic endeavor thanks to the National Defense Authorization Act of 2017, and in particular the codification of Title 10, Chapter 16, Security Cooperation.

Congress redefined nearly everything DOD does with a foreign partner as “security cooperation.” That definition includes not just exercises and information sharing—which is the traditional forte of operational forces—but the Army’s support of State Department-approved foreign military sales cases, direct commercial sales, the training provided to foreign partners at our schoolhouses and other programs as defined by Title 22 Security Assistance, a State Department authority executed by DOD.

Importantly, the new law mandates the creation of a formalized assessment, monitoring and evaluation efforts to foster more accurate and transparent reporting on the extent to which DOD achieves security cooperation outcomes and an evaluation of the reasons for success or lack thereof. This new accountability requirement intends to identify and disseminate best practices and lessons for security cooperation to inform decisions about policy, plans, programs and workforce. The law also requires an annual report to Congress on the measurable results of U.S. security cooperation investments.

Meanwhile, the Office of the Secretary of Defense for Security Cooperation issued assessment, monitoring and evaluation guidance as well as produced helpful guides such as “Standards and Guidelines for Security Cooperation Assessment,” which provide security cooperation programs and activities with standards, guidelines and tools to inform decision-making. Much of this new guidance places the task of assessing, monitoring and evaluating the security cooperation investment on the executing unit or agency, and the results are collected annually by the Office of the Secretary of Defense for Security Cooperation for a report to Congress.

MAJOR UPDATE

DOD publications updated as part of the National Defense Authorization Act of 2017:

· Department of Defense Directive 5132.03, “DOD Policy and Responsibilities Relating to Security Cooperation.”

· Department of Defense Instruction 5132.14, “Assessment, Monitoring, and Evaluation Policy for the Security Cooperation Enterprise.”

· Department of Defense Instruction 5132.15, “Implementation of the Security Cooperation Workforce Certification Program.”

The Defense Security Cooperation Agency’s comprehensive and expanded mission, according to the agency’s website, is “to advance U.S. defense and foreign policy interests by building the capacity of foreign partners in order to encourage and enable allies and partners to respond to shared challenges.” Important aspects of the agency’s mission are the tasks of managing and training the department’s security cooperation workforce and demonstrating the return on program investments, all while continuing to perform their traditional core functions such as defense trade and arms transfer, institutional capability building and international education and training. Much of that mission passes to each of the military services for execution through a variety of new guidance like that for workforce certification.

CONVERGING EFFORTS

Understandably, the new DOD and Defense Security Cooperation Agency guidance resulted in the Army rethinking top-to-bottom how it engages with foreign partners and manages its workforce. Specifically, the materiel side of international engagement, the Army security assistance enterprise, led by DASA (DE&C), began to collaborate more closely with the operational forces headed by the Army’s G-3/5/7. That synergistic effort resulted in the formulation of new Army guidance for the security cooperation enterprise that more closely aligns with “General Order 2020-01, Assignment of Functions and Responsibilities within Headquarters, Department of the Army,” and updated critical guidance in security cooperation-related Army regulations.

This refreshed Army policy marriage—operational security cooperation and security assistance—optimizes Congress’ 2017 guidance by contributing to the service’s combat readiness and the effectiveness of our security assistance efforts. Further, it ensures a whole-of-Army approach, which aligns plans that equip and train allies and foreign partners to better contribute to the Army Campaign Plan, the service’s guidance for allocating resources and tasks to satisfy the DOD mandates.

NEW REGS

Army publications created or updated in response to DOD changes:

· Army Regulation 11-31, “Army Security Cooperation Policy.”

· Army Regulation 12-1, “Security Assistance, Training, and Export Policy.”

· Army Regulation 5-22, “The Army Force Modernization Proponent System.”

The Army validated this new relationship with a number of significant administrative and strategy documents. In particular, those documents include the designation of the Army chief of operations and DASA (DE&C) as the Army’s force modernization co-leads for security cooperation. These partners also co-developed the Army Strategy for Allies and Partners and three of its annexes: Implementation of Security Cooperation with Allies and Partners, the Global Prioritization Assessment and Country Specific Guidance.

#### There is no part of the government not on board, it just takes a while

O’Mahony 18 Angela O’Mahony, associate dean for academic affairs at Pardee RAND Graduate School and a senior political scientist at RAND, former assistant professor of international political economy and economic statecraft at the University of British Columbia, PhD political science, UCSD; Ilana Blum, researcher at RAND; Gabriela Armenta, researcher at RAND; Nicholas Burger, senior economist at RAND and director of RAND’s Washington office; Joshua Mendelsohn, researcher at RAND; Michael J. McNerney, Acting Director, International Security and Defense Policy Center, and Senior International/Defense Researcher, at RAND, Affiliate Faculty at Pardee RAND Graduate School, MA international relations, University of Maryland; Steven W. Popper, researcher at RAND; Jefferson P. Marquis, Adjunct Political Scientist at RAND, PhD U.S. diplomatic and military history, Ohio State University, MA international security affairs, Columbia University; and Thomas S. Szayna, senior political scientist and former director of RAND's Defense and Political Sciences Department at RAND, MA international relations, Claremont Graduate School; “Assessing, Monitoring, and Evaluating Army Security Cooperation: A Framework for Implementation,” RR2165, RAND Corporation, 2018, <https://apps.dtic.mil/sti/pdfs/AD1056354.pdf> /GoGreen!

As Part I of this study discussed, Army security cooperation activities have aligned fairly well with what previous analyses have found contribute to effectiveness in both security cooperation and international development assistance. However, across the U.S. government, requirements for more rigorous and systematic AM&E are growing. The Army, with the rest of DoD, must improve its ability to analyze and report the extent to which its security cooperation activities are meeting their objectives. As Part I makes clear, there is still much to be learned. As the United States increases the scope of security cooperation, in terms of both activity and partner types, planners will need to understand not only what has been effective in the past but also how to identify lessons from the broader range of partners the United States is engaging. Part II of this study focuses on helping the Army develop an AM&E implementation framework that will better link security cooperation activities to their outcomes.

AM&E Developments—and Requirements—Are Accelerating

Within the past ten years, several developments have laid the foundations for a more strategic and analytically rigorous approach to security cooperation. As shown in Figure 4.1, these developments have arisen at several levels of government: Congress, the White House, OSD, DSCA, and combatant commands (CCMDs), and within the Army itself.

First, an important impetus for DoD’s recent efforts to improve the security cooperation AM&E process has come from Congress, some of whose members are eager for the department to improve its ability to track security cooperation resource expenditures and demonstrate the effectiveness of security cooperation programs in achieving DoD objectives at the national, theater, or country level. In Section 1202 of the Fiscal Year (FY) 2016 National Defense Authorization Act (NDAA), Congress mandated that DoD work with the Department of State (DoS) to establish a strategic framework for security cooperation “to guide prioritization of resources and activities.” Furthermore, it specified that one of the elements of this strategic framework would be “a methodology for assessing the effectiveness of Department of Defense security cooperation programs in making progress toward achieving the primary objectives, priorities, and desired end-states . . . including an identification of key benchmarks for such progress.”1 The FY 2017 NDAA reiterates the previous NDAA’s call for a security **[Figure 4.1 OMITTED]** cooperation AM&E framework, but goes further by requiring an “independent assessment of defense security cooperation programs.”2

Second, the National Security Council laid the groundwork in 2013 for a more integrated approach to security sector assistance. Directed primarily at DoS and DoD, Presidential Policy Directive 23 (Security Sector Assistance Policy) called for “a deliberate and inclusive whole-of-government process that ensures alignment of activities and resources with [U.S.] national security priorities.” Among other things, this meant ensuring greater consistency between programs and objectives, fostering transparency and coordination across U.S. government agencies, building sustainable partner security capacity through comprehensive sector strategies, being more selective in the use of security assistance resources to achieve the greatest impact, and informing policy with rigorous analysis, assessment, and evaluations. According to the directive, this latter effort would involve introducing “common standards and expectations for assessing security cooperation requirements” as well as “investing in monitoring and evaluation of security sector assistance programs.” Although the emphasis was on greater standardization of AM&E policies and procedures throughout the security assistance sector, the directive did indicate that newly established “standards and data collection will take into account the varying security and information environments where U.S. programs operate.”3

Third, in 2016 OSD released Department of Defense Instruction (DoDI) Assessment, Monitoring and Evaluation Policy for the Security Cooperation Enterprise, which provides guidance for a “whole of DoD” approach to security cooperation AM&E. It asserts that “accountability and learning are the primary purposes” of AM&E, and highlights AM&E’s importance in demonstrating security cooperation’s “returns on investment” so policymakers might “identify and improve or eliminate ineffective initiatives” as well as garner evidentiary support for policy and legislative proposals.4

The DoDI specifies two main military service requirements in supporting CCMD AM&E: (1) an initial (country-level) assessment of the security cooperation environment and (2) an initial design document (IDD) for “significant” security cooperation initiatives. “The initial assessment provides an understanding of the context, conditions, partner capabilities, and requirements immediately before the implementation of security cooperation initiatives and other activities.” It informs initiative design and establishes a “baseline against which to track progress.” The IDD contains milestones and measures that allow for performance monitoring and “independent and rigorous evaluations” of initiative “relevance, effectiveness, and sustainability.”5 The IDD must also include a TOC.

Within the terms of the DoDI, the GCCs have the primary security cooperation AM&E role. Their responsibilities include (1) leading initial assessment efforts, (2) orchestrating the assessment process, (3) formulating IDDs for all significant initiatives, (4) monitoring all significant initiatives, and (5) submitting to DSCA all initial country assessments and IDDs for new security cooperation initiatives.6 Based on the analysis in this report, services play an important role in every step of the AM&E process, particularly for the activities they implement directly. ASCCs play a particularly important role linking Army security cooperation to GCCs’ initial assessment and IDD.

In addition to issuing the DoDI, OSD has encouraged the development of AM&E processes, for example, by highlighting the importance of AM&E in various other guidance documents and hosting DoD-wide and interagency workshops to share best practices. These efforts were accelerated and better integrated after OSD’s establishment of a Deputy Assistant Secretary of Defense for Security Cooperation in 2015. This office undertook several initiatives over the past two years, supported by RAND’s National Defense Research Institute, which focused on institutionalizing best practices in security cooperation planning, transparency, and AM&E.7

Fourth, innovative concepts for using technology to improve data collection have allowed hundreds of U.S. security cooperation practitioners around the globe to report on their activities in more methodical and comprehensive ways and for policymakers and program managers to provide more rigorous oversight. The creation of security cooperation management information systems by the GCCs and other DoD organizations provided unprecedented platforms for planning, resourcing, assessing, monitoring, and evaluating future security cooperation AM&E efforts. These largely independent initiatives have begun to coalesce in the form of a comprehensive tool for tracking DoD security cooperation activities and resources: G-TSCMIS, whose development is being managed by DSCA (with support from the Joint Staff) and is required to be used by all DoD security cooperation activity managers. G-TSCMIS is still a work in progress, and CCMDs face challenges getting all relevant activities included in the system.8 Still, even when G-TSCMIS is fully developed and widely used, it will not fulfill all the information management needs required for effective security cooperation planning and AM&E, which is why the CCMDs and other security cooperation organizations continue to use their own systems.

In addition to overseeing the development of G-TSCMIS, DSCA has also recently launched an initiative to formalize security cooperation workforce competencies and associated experiential and training requirements, which could eventually contribute to a larger pool of qualified AM&E professionals within the security cooperation field.

Fifth, the Joint Staff has also played an important role in attempting to improve and standardize security cooperation and security force assistance (SFA) doctrine, including with respect to AM&E. Acknowledging the challenge of determining the extent to which security cooperation activities have contributed to U.S. objectives, the draft Joint Publication 3-20 provides guidelines for three kinds of security cooperation assessments: operations assessments (which focus on “are we doing the right things”), task assessments (which focus on “are we doing things right”), and functional assessments (which focus on “are we efficient and effective”).9

Sixth, OSD established theater campaign plans (TCPs) for CCMDs and campaign support plans for the military services as a way of applying military planning techniques beyond traditional war plans to incorporate more steady-state activities like security cooperation. These plans allowed for a Secretary of Defense–led analysis and discussion of security cooperation ends, ways, and means that did not exist before. More recently, the CCMDs have begun to develop country plans that promise a clear auditing trail between theater objectives and the means (activities and resources) employed to achieve them that involve U.S. allies and partner nations, given appropriate country objectives and metrics as well as improved country-level data collection.