# Research

## Research Terms

**Best hits:** “distraction”

current nato cooperation initiatives

“traditionalists” vs “wideners”

“nato” “out of area” operations

“"offensive cyber operations"AROUND(5) -less expensive”

“nato strategic concept”

nato climate strategy

NATO “Climate Change and Security Centre of Excellence”

Current initiatives

**Cyber**

nato cooperative cyber defense center of excellence

"NATO" "cyber" "funding shortfall"

<https://www.npr.org/2022/05/02/1095008257/estonia-nato-cyber-war-games-russia>

[Cooperation and exercises key to cyber defence, says Nato centre (computerweekly.com)](https://www.computerweekly.com/news/252436575/Cooperation-and-exercises-key-to-cyber-defence-says-Nato-centre)

**Climate**

“nato” “climate” “distraction”

[NATO Needs Realistic Goals Toward Russia - Carnegie Europe - Carnegie Endowment for International Peace](https://carnegieeurope.eu/strategiceurope/65041)

# Neg

Clearing house infosharing link

Nato not doing info sharing now,

## Priorities

Make CP file,,

DA

* Infos-sharing link
* AT: link turn

### Cites

"Major Power Failures Hit Brazil." BBC News,2009.

The United States Strategic Bombing Surveys, Summary Report. Maxwell Airforce Base,

Alabama: Air University Press, 1945.

Adams, James. "Virtual Defense." Foreign Affairs 80, no. 3 (2001).

———. "Virtual Defense." Foreign Affairs (2001).

Albright, David. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?

Preliminary Assessment." ISIS Reports (2010).

Arendt, Hannah. On Violence. New York: Harcourt, Brace, 1970.

Blainey, Geoffrey. The Causes of War. New York: Free Press, 1973.

Borg, S. "Economically Complex Cyber Attacks." IEEE Security and Privacy 3, no. 6 (2005).

Clover, Charles. "Kremlin Backed Group Behind Estonia Cyber Blitz." Financial Times- Europe

(2009).

Devost, Matthew and Neal Pollard. "Taking Cyber-Terrorism Seriously." Terrorism Research

Centre (2002).

Gartzke, Eric. "The Myth of Cyberwar." International Security 38, no. 2.

Goodman, Will. "Cyber Deterrence." Strategic Studies Quarterly (2010).

Gray, C. S. Another Bloody Century, Future Warfare. London: Phoenix, 2005.

Hart, Liddell. Strategy. New York: Penguin Books, 1991.

Hesseldahl, A. "Computer Worm may be Targeting Iranian Nuclear Sites." Bloomberg (2010).

Jackson, William. "Fuss Over Cyber War Distracts from Real Threats, Security Pioneer Says."

Gcn (2012).

Joint Publication 3-13, Joint Doctrine for Info Ops (2006).

Kirschner, S. "I Love You...Not." Popular Science. (2000).

Krepinevich, Andrew. "Cyberwarfare: A "Nuclear Option"?" Centre for Strategic and Bugetary

Assessments (2012).

Kuehl, Daniel. "From Cyberspace to Cyberproblem: Defining the Problem." In Cyberpower and

National Security. Vol. 48, 2009.

Langner, R. Cracking Stuxnet: A 21st Century Cyberweapon. Anonymous 2011. (Ted.com).

27

Lee, M. and L. Hornby. "Google Attack Puts Spotlight on China's "Red" Hackers." Reuters

(2010).

Libicki, Martin. Conquest in Cyberspace Cambridge University Press, 2007.

———. "Why Cyber War Will Not and should Not have its Grand Strategy." Strategic Studies

Quarterly (2014).

Liff, A. "Cyberwar: A New Absolute Weapon? the Strategic Proliferation of Cyberwarfare

Capabilities and Interstate War." War of Strategic Studies 35, no. 3 (2012).

Lin, Patrick. "Is it Possible to Wage just a Cyberwar?" The Atlantic (2012).

Loeb, Vernon. "Pentagon Computers Under Assault." Washington Post,2001.

Lucas, George R. "Postmodern War." Journal of Military Ethics 9, no. 4 (2010).

Lupovici, A. "Cyber Warfare and Deterrence: Trends and Challenges in Research." Military and

Stategic Affairs 3, no. 3 (2011).

Maurer, Tim. "The Case for Cyberwarfare." Foreign Policy (2011).

McGlaun, Shane. "DARPA Wants More Money for Cyber Weapons." Daily Tech Magazine

(2011).

Messick, Graham. "Cyber War: Sabotaging the System." CBS News,2009.

Nakashima, Ellen. "Defense Officials Discloses Cyberattacks." The Washington Post,2010.

———. "US Cyberweapons had been Considered to Disrupt Gaddafi's Air Defenses." The

Washington Post,2011.

Nazario, Jose. "Politically Motivated Denial of Service Attacks." Arbor Networks.

Nye, J. "Cyber Power." Belfer Centre for Science and Int'l Affairs Harvard Kennedy School

(2010).

O'Donnell, B. T. "Humanitarian Law:Developing International Rules of The Digital Battlefield."

Journal of Conflict and Security Law 8, no. 1 (2003).

Office of the Chairman, Joint Chiefs of Staff. National Military Strategy. Washington, D.C:

1997.

Rantanen, Miska. "Virtual Harassment, but for Real." Helsingin Sanomat (2007).

Rid, Thomas. "Cyber War Will Not Take Place." Journal of Strategic Studies 35, no. 1 (2012).

———. Cyber War Will Not Take Place. London: Hurst and Company, 2013.

———. "Cyberwar and Peace." Foreign Affairs (2013).

Rid, Thomas and Peter McBurney. "Cyber-Weapons." Rusi Journal 157, no. 1 (2012).

28

Rowe, Neil. "The Ethics of Cyberweapons in Warfare." International Journal of Cyberethics 1,

no. 1 (2009).

Rustici, Ross. "Cyberweapons: Leveling the International Playing Field." Strategic Studies

Institute (2011).

Schmitt, M. "Wired Warfare: Computer Network Attack and Jus in Bello." International Review

of the Red Cross 84, no. 846 (2002).

Schneier, Bruce. "Want to Evade NSA Spying? Don't Connect to the Internet." Wired (2013).

Schreier, Fred. "On Cyberwarfare." DCAF Horizon (2015).

Sommer, Peter. "Experts Say, Iran has Neutralized Stuxnet." YNet News- Middle East (2012).

Suciu, Peter. "Why Cyberwarfare is so Attractive to Small Nations." Fortune Magazine (2014).

UNSC Resolution 1113 (2011).

von Clausewitz, Carl. On War. New York: Oxford University Press, 1976.

Weimann, Gabriel. "Cyberterrorism: How Real is the Threat?" USA Institute of Peace (2004).

Weinberger, Sharon. "How Israel Spoofed Syria's Air Defence System." Wired (Oct 2007).

# CP – EU

# CP – Bilat

### Strategic case D

Current OCOs sufficient to deter Russia

No follow on

* have internal link and impact defense to Russia low level cyber

u r wrong that there is fratricide

cohesion OK now DESPITE alt causes to mistrust

Hybrid war naur escalate

### To cut

~~AT: L2NB~~

t/c

AT: turns

### Notes

“NATO bilateral intelligence sharing”

US unilaterally – disclosing without security coop

US bilaterally do OCOs with NATO member countries

US do unilat things that solve internal links/impacts

Reduce fratricide

Smooth stuff over w/ allies

Proportionate response options that is not cyber

Process

* Look at internal links
* Adv cp stuff later

-----

* Ask bk about info sharing bw non-US allies
* This card possible answer?

### 1NC – CP

#### The United States federal government should substantially increase its bilateral cooperation with the member states of the North Atlantic Treaty Organization through establishing an interoperable network for information sharing regarding its offensive cyber operations and capabilities.

#### Bilateral intel-sharing solves best – controlled cooperation overcomes gaps in perception and capability.

Ballast, '17 – Jan Ballast MA is a senior staff member, involved with foreign intelligence, mission support and national security, working for the Ministry of Defence of The Netherlands. He has held numerous analytical and operational positions in both The Hague and missions abroad. The views expressed here are the author’s and do not necessarily reflect the official position of the Government of The Netherlands or any of its departments or agencies (Jan Ballast; "Trust (in) NATO The future of intelligence sharing within the Alliance"; No Publication; https://rieas.gr/images/rieasnews/NATOarticle17.pdf; 09-2017, Accessed 6-25-2022)//ILake-NoC

Sharing secrets

To outsiders (counter)intelligence – the (often covert) collection, analysis, sharing and operationalization of sensitive information of military or political value – is shrouded in mystery.7 Non-intelligence personnel always find it hard to fathom why joint operations, return on investment and comprehensive approach leave their intelligence colleagues with eyes glazed over. They are ignorant of intelligence’s obscure characteristics such as trust, risk mitigation, national interest, deception and quid pro quo. For instance, intelligence is a trade-off between trusting a partner enough to share information that could endanger one’s own source, against the benefits of doing so. In the protection of national interest allies are deceived and intelligence cooperation is carefully weighed even with partners (quid pro quo, meaning ‘tit for tat’). This section of the paper outlines why reluctant attitudes to multilateral exchange will remain pivotal in intelligence.

Intelligence is, as a rule, executed by national (civilian, military and hybrid) intelligence and security services that use a combination of intelligence sources to answer Priority Intelligence Requirements (PIRs) of national operational commanders and other decision-making authorities. In the collection process, open sources set the information stage, whereas secret intelligence tends to explain the behavior of the main actors.8 States and their national services are reluctant to share sensitive, classified information with international organizations and favor cooperation on a more controllable, bilateral, case-by-case basis.9 In fact, intelligence is shared only when there is a common threat perception, mutual trust, a demonstrable added value, the right type of diplomatic relationships or a combination of incentives.10 The most successful bilateral secret intelligence collaboration is the AngloAmerican UKUSA Agreement, originally signed in 1946, which evolved into the exclusive multilateral so-called ‘Five Eyes’ cooperation.11

Examples of beneficial intelligence cooperation by states within international organizations, such as NATO, are much harder to find. Friedrich Korkisch noted that during the last decades of the twentieth century, intelligence within the Alliance was “the result of the early years of NATO, when it was assumed that all NATO forces would remain under national command, and strategic intelligence would be mainly national intelligence.”12 From the outset Member States shared secret information bilaterally on political and military issues with NATO; however, major countries within the Alliance, afraid of the non-secure Brussels apparatus, kept intelligence from other Members.13 Chris Clough warned that, “within recent military coalitions, intelligencecontributing nations have been mindful of the dangers of compromise by less security-conscious partners, while knowing that a degree of sharing is essential.”14 Some argue that international institutions like NATO play a major role in encouraging and facilitating intelligence sharing among their member states.15 Although, “even in the UN intelligence is no longer a dirty word,”16 others remain of the opinion that nations are unable to overcome mistrust, making them reluctant to engage in multilateral intelligence cooperation.

The focus of the intelligence world changed profoundly following 9/11 with the emergence of counterterrorism (CT) and non-state actors as dominating global themes.18 Nations witnessed the introduction of collection coordinating mechanisms, such as the Office of the Director of National Intelligence (ODNI) in the United States,19 and target-oriented intelligence fusion centers, such as the Joint Terrorism Analysis Center (JTAC) in the UK.20 Due to the perceived common threat, bilateral exchange of intelligence intensified and alignments were formed even with non-traditional partners. Although this new collaboration with states in Africa and the Near, Middle and Far East resulted in challenges in the realms of oversight and human rights, access to raw data and insights on CT was deemed too relevant not to engage – ‘gains’ outweighed ‘risks’.21 Following the terrorist attacks on major European cities, cooperation between the security services deepened and nations realized that solidarity as well as sharing intelligence on CT should be the norm.22

On a multilateral level, NATO, lacking its own sources by design, responded by introducing intelligence liaison and fusion elements and reaffirmed its commitment to intelligence sharing.23 However, different languages, cultures, capabilities and infrastructures proved to be structural constraints.24 Unlike the Alliance, the leadership of the European Union (EU) claimed a coordinating role in support of all state-level courses of action on CT through a combination of its law enforcement agency Europol, judicial cooperation agency Eurojust and border management agency Frontex.25 The EU, not questioning state actors as first responders to terrorism and its related criminal networks, strengthened its intelligence structure and joint multilateral intelligence collaboration was suggested.26 John Nomikos noted that “while Belgium, [The Netherlands] and Austria demanded a CIA-style EU agency, powerful member states including Britain, Germany, France, Spain and Italy showed a reluctance to share intelligence.”27 Following the Paris 2015 attacks, German Interior Minister Thomas de Maizière shattered Belgian, Dutch and Austrian dreams; “We should not focus our efforts on creating a new European intelligence service now. I cannot imagine we will be willing to give up our national sovereignty.”2

### 1NC – Jones

#### The United States federal government should

#### make blunt and regular warnings to Russia that their information campaign will be met with equally forceful response;

#### further invest in offensive cyber operations to deter Russia.

**The threat of US OCOs alone sufficiently deters Russia.**

**1AC Jones 18** – Harold Brown Chair and Director of the Transnational Threats Project at the Center for Strategic and International Studies (CSIS) Seth G. Jones, “Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare,” Center for Strategic & International Studies, October 2018, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181002\_Russia\_Active\_Measures\_FINAL1.pdf

It is important to play defense—including protecting U.S. and allied cyber networks, exposing Russian bots and trolls, and preparing for cyberattacks and disinformation. But Russia will **continue to target** the United States at home and abroad until the U.S. government **implements** a **more aggressive offensive information campaign**. The goal should be to **coerce Russia** to **curb** its **information warfare campaign**, **punish Moscow** when these incidents occur, and **exploit** Moscow’s **weaknesses** and **vulnerabilities**. An offensive U.S. campaign might include several steps. The first involves blunt and regular U.S. warnings to Russian leaders, both in public and private, that their information warfare campaign will be met with an equally forceful response. Senior U.S. officials like President Donald Trump have not seriously threatened Moscow despite substantial evidence of Russian activism in the 2016 U.S. elections; Russian efforts to exploit issues like gun control, Black Lives Matter, and the #MeToo movement; and cyberattacks against even conservative U.S. organizations like the Hudson Institute and the International Republican Institute. Following the Soviet Union’s global active measures campaign against the United States, U.S. President Ronald Reagan vowed to respond in kind and, ultimately, to “leave Marxism-Leninism on the ash-heap of history.” Moscow understood that Reagan and his administration were deadly serious about combating Russian active measures, which is what Reagan did in authorizing effective overt and covert action programs against the Soviet Union. Second, the United States needs to continue developing its offensive cyber capabilities and—just as important—it needs to **use them if necessary**. President Trump’s decision to sign National Security Presidential Memorandum 13, a directive facilitating offensive U.S. cyber operations, is a helpful step. This directive rescinded the Obama administration’s more cautious approach under Presidential Policy Directive 20.46 But this change **means little** if the U.S. **fails to use**—or, more importantly, to **threaten to use**—**cyberattacks** to **protect itself** from **cyber operations** by countries like Russia. In his influential work “Arms and Influence,” the Nobel Prizewinning economist Thomas Schelling wrote that “it is the threat of damage, or of more damage to come, that can make someone **yield** or **comply**.” Moscow needs to understand that the United States is **prepared** to **use all available instruments**—**including cyber operations**—if it continues to be threatened.

## 2NC – Solvency

Solves mistrust

How to explain that it overcomes fratricide.

### 2NC – S – T/L

#### Bilateral cyber partnerships already exist and guarantee an interoperable cyberspace.

Williams, '21 – Brandon Kirk Williams is a postdoctoral research fellow at the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory Center for Global Security Research (Brandon Williams; "U.S. and Allied Cyber Security Cooperation in the Indo-Pacific"; Lawrence Livermore National Laboratory; https://cgsr.llnl.gov/content/assets/docs/US\_and\_Allied\_Cyber\_Security\_Cooperation\_in\_the\_Indo-Pacific.pdf; 04-01-2021, Accessed 6-27-2022)//ILake-NoC

The Transatlantic relationship illustrates the complexities of cyber security cooperation. The United States, NATO, and the European Union (EU) share common ground based on decades of partnership across issue areas. All parties agree on the necessity of a free, open, and interoperable cyberspace free from authoritarian state control. NATO members declared that collective defense—enshrined in Article 5 of the NATO Status of Forces Agreement—applies in cyberspace. Within NATO, the United States supports NATO’s Cooperative Cyber Defence Centre of Excellence (CCDCOE) and support for cyber missions. Separately from NATO, the United States retains strong bilateral cyber security partnerships with EU member states. USCC conducted Hunt Forward missions in EU nations to glean intelligence on malicious cyber activities.

#### That’s key to tailor to country-specific needs.

Williams, '21 – Brandon Kirk Williams is a postdoctoral research fellow at the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory Center for Global Security Research (Brandon Williams; "U.S. and Allied Cyber Security Cooperation in the Indo-Pacific"; Lawrence Livermore National Laboratory; https://cgsr.llnl.gov/content/assets/docs/US\_and\_Allied\_Cyber\_Security\_Cooperation\_in\_the\_Indo-Pacific.pdf; 04-01-2021, Accessed 6-27-2022)//ILake-NoC

Key lessons emerge from assessing progress in the Transatlantic cybersecurity experience. Europe’s foundation for cybersecurity cooperation began in recent years. CCDCOE regularly assists Australia and Japan, and South Korea partners with the EU’s Malware Information Sharing Platform. The EU and NATO took the lead on responding to the request for cyber capacity by Indo-Pacific allies. Panelists concluded the United States and Europe must respect that local context triggers country-specific demand signals. The United States can commit to dialogue that will tailor solutions to country-specific needs. Countering APTs may take time. CCDCOE exercises and capacity building missions demonstrated that knowing local context sets a baseline, and one that will be essential for changing the perception of the cyber threat ecosystem and the solutions necessary to confront adversaries in cyberspace.

#### Bilateral collaboration solves better – NATO cyber resources are stretched too thin.

Pernik, '21 – Piret Pernik is a researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). She has researched cybersecurity strategic and policy aspects since 2013. She has published research reports and analyses on cyber resilience, military 5G security, cyber commands, and cyber defence training (Piret Pernik; "Cyber deterrence: A case study on Estonia’s policies and practice"; Hybrid CoE; https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012\_Hybrid\_CoE\_Paper\_8\_Cyber\_deterrence\_WEB.pdf; 10-2021, Accessed 6-27-2022)//ILake-NoC

Based on the Estonian case study, a policy recommendation for EU and NATO countries is to apply a three-layered deterrence model.73 First, EU and NATO countries should participate in entanglement and norms measures such as cyber diplomacy and capacity-building globally. Second, they should invest more in denial measures and, third, jointly develop policies for punitive response options, including developing public attribution procedures to enable quick attribution, and systematically implementing sanctions regimes. It would be feasible to establish memoranda of understanding, and operational- and technical-level frameworks to radically improve information- and intelligence-sharing. Participation in cyber defence and crisis management exercises should be open to like-minded NATO partner countries. Joint bilateral cyberspace operations likewise contribute to mutual trust-building and information-sharing, and increase parties’ operational and technical competence.74 Operational- and technical-level joint activities should be regularly practised among allies and with like-minded partners as they contribute to deterrence by denial. Given that NATO’s cyber response teams are stretched thin due to protecting NATO’s own networks, bi- and multilateral collaboration enables countries to share best practices and, in the event of an emergency, to provide mutual rapid assistance in crisis response.

### 2NC – S – Trust\*

### 2NC – S – Interoperability

#### The CP uses bilateral interoperability roadmaps to streamline SC broadly.

O’Mahony et al., '22 – associate dean for academic affairs at Pardee RAND Graduate School and a senior political scientist at RAND (O'Mahony, Angela, David E. Thaler, Beth Grill, Jennifer D. P. Moroney, Jason H. Campbell, Rachel Tecott, and Mary Kate Adgie; "Prioritizing Security Cooperation with Highly Capable U.S. Allies: Framing Army-to-Army Partnerships"; RAND Corporation; https://www.rand.org/content/dam/rand/pubs/research\_reports/RRA600/RRA641-1/RAND\_RRA641-1.pdf; 2022, Accessed 6-27-2022)//ILake-NoC

Security Cooperation to Expand Interoperability Is a Strong Focus of U.S.-Allied Military Relationships

Allies such as the United Kingdom and Australia support and encourage interoperability discussions and new investments during senior-level interactions with the Army. For example, interoperability discussions have historically dominated the agenda for the U.S.-British army-to-army staff talks. The Multinational Fusion Cell in the HQDA brings together assigned personnel from multiple allied countries (the United Kingdom, Australia, Japan, Germany, France, and others) to focus on interoperability and to develop U.S.-allied bilateral interoperability roadmaps. Standing organizations, such as ABCANZ, also exist to work through interoperability issues at the operational level. Large-scale exercises, such as the aforementioned biannual Talisman Sabre series between the United States and Australia, are very much focused on addressing interoperability challenges identified from recent operations and planning for future operations. NATO defines interoperability along three dimensions—human, procedural, and technical—which is a helpful way to categorize interoperability challenges.34 We find general agreement among our interlocutors that SC with highly capable allies to support human, procedural, and technical interoperability is advancing at the operational and tactical levels, but there is concern about a lack of multiyear funding and programming to guide longer-term planning for multinational interoperability exercises.35

Despite this focus, interoperability initiatives at the strategic level have been relatively ad hoc from allies’ perspectives. The Army’s Interoperability Campaign Plan frames and institutionalizes interoperability efforts internally and operationalizes it with designated partners. Allies support the Army’s focus on interoperability writ large, but the links between interoperability planning and ongoing SC activities needs to be stronger. As an example, the GORT, a bilateral event between the United States and the United Kingdom at the three- and four-star level, is not explicitly linked to the discussions that occur at the one- and two-star levels. According to key allied officials, issues raised at the GORT level should be automatically addressed at the subsequent Army staff talks (ASTs) and drive the discussions at the lower level working groups. Interoperability issues and priorities raised at the GORTs/staff talks should also be linked to other key bilateral SC activities, creating a real battle rhythm for interoperability.

Moreover, allies have suggested that although bilateral vision statements for interoperability—such as the emerging one with the United Kingdom— are positive steps, their language could be made stronger and clearer. They suggest dropping the term vision and making bilateral campaign plans. In addition, aspirational verbs in Army plans, such as institutionalize, should be replaced by stronger verbs, such as guarantee.

Both British and Australian officials talk about wanting to be the United States’ partner of choice; the United Kingdom has in place an explicit strategic communications campaign plan that focuses on improved access and science and technology collaboration. For the United Kingdom, this partnering includes such areas as energy; antisubmarine warfare; hypersonics; network command, control, and communications; and nuclear collaboration. For Australia, areas include intelligence, surveillance, and reconnaissance; radars; and other high-technology systems. The emphasis on being a partner of choice refers to being capable, likeminded, and committed. It is understandable why key allies desire to have the strongest language possible in interoperability planning documents.

Implications

We derived the following implications from our findings on expanding interoperability with the United Kingdom, Australia, and other highly capable allies:

• Strengthening the links between key SC activities focused on interoperability at the top level to lower echelons will help to ensure that the messages are clear and that appropriate actions are taken at the working group levels. In this area formal mechanisms for linking the deliberations and decisions made at GORT meetings with activities at the army-to-army staff talks would be helpful.

• Language in interoperability planning documents could be less aspirational and more definitive. Not only would this make SC plans for interoperability more concrete for both the United States and its allies, but it would also encourage formulation of measurable goals and metrics for the SC community to enable assessment, monitoring, and evaluation of progress in enhancing that interoperability.

### 2NC – S – Follow-On

#### Only bilateral cooperation ensures multi-way info sharing – ensures adjusted burden sharing based on a state’s domestic priorities.

Gressel, '19 – senior policy fellow with the Wider Europe Programme at the European Council on Foreign Relations' Berlin office (Gustav Gressel; "Protecting Europe against hybrid threats"; ECFR; https://ecfr.eu/publication/protecting\_europe\_against\_hybrid\_threats/; 6-25-2019, Accessed 6-27-2022)//ILake-NoC

The activities of Russian intelligence services increasingly pop up in public security debates. In some cases, the known activities of Russian operatives involve classical espionage. In others, their activities hint at much more robust subversive aims: cultivation of anti-system forces, the purchase and preparation of infrastructure for future military incursions, training for paramilitary resistance groups, and the assassination of perceived enemies. These actions are top-tier covert actions. One may assume that other actions that provide the basis for this sort of activity – such as strategic reconnaissance, cyber penetration and espionage, excavation of data, the placement agents in positions of power, and reconnaissance of critical infrastructure – have progressed as well. Europe has a mixed record of disrupting these preparations.

While EU member states on the eastern flank have adopted very robust counter-intelligence laws and invested significant resources in monitoring Russian operatives, other states are more reluctant to do so. France has the legal framework for such action, but counter-terrorism is its first priority. Germany and Austria – both countries that were under Allied supervision and occupation after 1945 – have comparatively weak laws, and their decision-makers maintain a ‘hands-off’ mentality. In the past, bilateral cooperation with US services addressed these imbalances. As a legacy of the post-war situation, US and British services have the right to engage in counter-intelligence work in Germany. And Berlin, which has historical issues with counter-intelligence, has been happy to outsource this politically toxic work. In doing so, Washington – and to a lesser extent London – became an external balancer in intra-European affairs. And while the Trump administration and its sometimes erratic personnel have significantly undermined confidence in the US government, the US intelligence community has remained much more stable and able to preserve working contacts throughout Europe. But if relations with Washington deteriorate further, there is no tangible policy or political actor that could replace the US.

### 2NC – S – Coordination/Integration

#### Solves coordination through crafting bilateral diplomatic channels – that establishes a broad consensus for cyberspace policies.

Goldman, '20 – Emily Goldman is Director of the US Cyber Command / National Security Agency Combined Action Group. (Emily O. Goldman; "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy"; Texas National Security Review; https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/; 09-03-2020, Accessed 6-27-2022)//ILake-NoC

Communicate and Build Consensus

The State Department’s foreign service officers forward-deployed as “cyber diplomats” can strengthen consensus among allies and partners on the nature of the cyber security problem and on the need for action to address it. To do so, they should be conversant with the U.S. government’s efforts to address cyber competition and armed with information to speak authoritatively about them. The State Department has long promoted a framework for responsible state behavior in cyberspace. The key elements of that framework include: (1) affirmation that established principles of international law apply to state behavior in cyberspace;62 (2) adherence to certain non-binding norms of state behavior in cyberspace during peacetime; and (3) consideration, development, and implementation of practical confidence-building measures to reduce the risk of conflict in cyberspace. Since not all states share American views on responsible behavior in cyberspace, the United States is working with partners and allies on collective attribution and imposition of consequences.

These initiatives are now being complemented by the Department of Defense’s strategy of defend forward and U.S. Cyber Command’s operational approach of persistent engagement. The State Department and United States Agency for International Development (USAID) officers in missions around the world need to be well-versed in these other efforts and prepared to explain them to foreign partners on a routine basis. America’s partners want to understand U.S. government strategy and policies.63 It is U.S. policy that cross-domain responses to cyber aggression should be complemented with steady and sustained activities to make networks more resilient, to defend them as far forward as practicable, and to contest the most dangerous adversaries.64 Every diplomatic engagement that includes cyber issues would be an opportunity to build support for these mutually reinforcing approaches.

Bolster Cyber Cadre

The greatest talent, most consequential research and development, and most innovative applications of cyber and other emerging technologies are globally distributed across individuals, commercial entities, governments, and academia. Competing successfully requires recognizing, understanding, and leveraging insights and advances wherever they reside in real time. The nation that best understands and can most rapidly harvest the benefits of changing knowledge (e.g., quantum encryption, artificial intelligence, machine learning, high performance computing, big data, 5G) will be best positioned to secure its future. Conversely, states that lag behind competitors will find closing gaps a daunting and risky challenge. 5G represents the proverbial canary in the coal mine because the United States lags behind China in deployment. Unless the United States ensures the talent is in place to monitor and lead on future technologies, it may again be caught unprepared.

The State Department does designate foreign service officers with a cyber portfolio, but they are usually assigned as an additional duty, often to economic officers at embassies and consulates. One option would be a dedicated cadre of “cyber diplomacy-coned” officers,65 or even a regional dedicated officer cadre located at a large or strategic embassy in each region to augment the part-time officers at post. These cyber diplomacy-coned foreign service officers would report on priorities and trends in research and investments across governments, industries, academia, and research institutes worldwide, and identify where adversary regimes are vulnerable to diplomatic, information, military, and economic threats.66 They would “identify and catalyze opportunities,” in the words of the U.S. National Security Strategy,67helping to set the conditions for competition by building mechanisms for information sharing and agile collaboration.

Enable Defend Forward

The U.S. National Cyber Strategy’s guidance to promote a framework of responsible state behavior in cyberspace, one that ensures there are consequences for irresponsible behavior, is a key objective for the United States. To succeed, this framework should be pursued in tandem with an active approach to stem ongoing adversary cyberspace campaigns outside of armed conflict. The Department of Defense is now defending forward, outside its existing networks, to mitigate threats before they reach the United States. It is time for the State Department to join in these efforts.

An informal division of labor currently exists between the departments of State and Defense, whereby the former promotes norms in traditional diplomatic channels while the latter pursues defend forward through military channels. Yet this leaves several problems unresolved. Parallel communication increases the risk of messaging fratricide across military and diplomatic channels in partner nations. Military cyber operations may engage foreign policy sensitivities that the State Department is better equipped to address. On the other hand, State Department desk officers may throw a wrench into planning because they do not understand Defense Department strategy.

The United States needs to operate continuously alongside allies and partners. Leadership from the State Department can increase the speed, agility, and scale of defend forward activities and operations by working through diplomatic channels to set the conditions for the United States to operate by, with, and through foreign partners and their networks in order to expose, contest, and defend against adversary cyber aggression. Sustained diplomacy can help institutionalize these operational partnerships and make defend forward more anticipatory and effective. Institutionalized cooperation, including the conduct of joint and coalition operations and the development of agreed-upon legal and policy frameworks, is essential to prevail in long-term strategic competition.

Leadership from the State Department can increase the speed, agility, and scale of defend forward activities and operations...

The State Department can set the conditions for consensual foreign partner-enabled discovery operations (i.e., “hunt forward” operations) through bilateral engagements.68 These operations enable the United States and its partners to understand an adversary’s tactics, techniques, and procedures. This will in turn enable network defense of U.S. partners, improve anticipatory resilience of U.S. and partner networks, and thwart cyberspace aggression. The State Department can scale the process of explaining the Defense Department’s defend forward strategy, enabling the United States to proactively set the conditions for “hunt forward” operations. The State Department can also actively ensure Defense Department cyber teams receive support from U.S. embassy country teams and benefit from insights about foreign partner networks gained through State and USAID-led cyber security capacity-building programs.

## 2NC – NB

### 2NC – AT: L2NB – Tradeoff

#### Resources are deliberately allocated for NATO and do not blur with a member state’s general budget for domestic spending.

NATO, ‘22 – NATO. ("Funding NATO "; NATO; https://www.nato.int/cps/en/natohq/topics\_67655.htm; 04-01-2022, Accessed 6-28-2022)//ILake-NoC

Allocation and control of common-funded resources are decided by consensus among Allies. Under the overall authority of the North Atlantic Council (or NAC), various bodies exercise managerial control over the four principal elements of the Organization’s financial structure:

the International Staff, financed by the civil budget;

the international military structure, financed by the military budget;

the NSIP; and

NATO agencies.

When cooperative activities do not involve all member countries, they are for the most part managed by NATO production and logistics programmes within NATO agencies. They have their own supervisory boards and boards of directors, as well as finance committees and distinct sources of financing within national treasuries.

Financial control

With respect to the military and civil budgets, the head of the NATO body is ultimately responsible for the correct preparation and execution of the budget. The administrative support for this task is largely entrusted to the financial controller of the agency or NATO body.

Each financial controller has final recourse to the Budget Committee in case of persistent disagreement with the head of the respective NATO body regarding an intended transaction. The financial controller is charged with ensuring that all aspects of execution of the budget conform to expenditure authorisations, to any special controls imposed by the Budget Committee, and to the financial regulations and their associated implementing rules and procedures. He may also, in response to internal auditing, institute such additional controls and procedures as he deems necessary for maintaining accountability.

International Board of Auditors for NATO

The independent International Board of Auditors for NATO (IBAN) is responsible for auditing the accounts of the different NATO bodies. Its principal task is to provide the NAC and member governments with the assurance that joint and common funds are properly used for the settlement of authorised expenditure and that expenditure is within the financial authorisations granted.

## 2NC – Perm

### 2NC – AT: PDB

#### 1) Links to tradeoff

Dpublication DA

### 2NC – AT PDCP

#### NATO is the military alliance---to be considered a NATO activity, NATO itself must be the initiating or joint initiating authority.

NATO 22, “ABOUT NATO,” US Mission to the North Atlantic Treaty Organization, <https://nato.usmission.gov/about-nato/>

Formed in 1949 with the signing of the Washington Treaty, NATO is a security alliance of 30 countries from North America and Europe. NATO’s fundamental goal is to safeguard the Allies’ freedom and security by political and military means. NATO remains the principal security instrument of the transatlantic community and expression of its common democratic values. It is the practical means through which the security of North America and Europe are permanently tied together. NATO enlargement has furthered the U.S. goal of a Europe whole, free, and at peace.

Article 5 of the Washington Treaty — that an attack against one Ally is an attack against all — is at the core of the Alliance, a promise of collective defense. Article 4 of the treaty ensures consultations among Allies on security matters of common interest, which have expanded from a narrowly defined Soviet threat to the critical mission in Afghanistan, as well as peacekeeping in Kosovo and new threats to security such as cyber attacks, and global threats such as terrorism and piracy that affect the Alliance and its global network of partners.

In addition to its traditional role in the territorial defense of Allied nations, NATO leads the UN-mandated International Security Assistance Force (ISAF) in Afghanistan and has ongoing missions in the Balkans and the Mediterranean; it also conducts extensive training exercises and offers security support to partners around the globe, including the European Union in particular but also the United Nations and the African Union.

MEMBER STATES

The NATO Alliance consists of 30 member states from North America and Europe. Article Five of the treaty states that if an armed attack occurs against one of the member states, it should be considered an attack against all members, and other members shall assist the attacked member, with armed forces if necessary.

List of Member States

Over the past two decades, the Alliance has developed a network of structured partnerships with countries from the Euro-Atlantic area, the Mediterranean and the Gulf region, as well as individual relationships with other partners across the globe. NATO pursues dialogue and practical cooperation with many partner countries and engages actively with other international actors and organisations on a wide range of political and security-related issues.

List of NATO Partners

STRUCTURE

NATO is comprised of two main parts, the political and military components. NATO Headquarters is where representatives from all the member states come together to make decisions on a consensus basis. It also offers a venue for dialogue and cooperation between partner countries and NATO member countries, enabling them to work together in their efforts to bring about peace and stability.The key elements of NATO’s military organisation are the Military Committee, composed of the Chiefs of Defence of NATO member countries, its executive body, the International Military Staff, and the military Command Structure (distinct from the Force Structure), which is composed of Allied Command Operations and Allied Command Transformation, headed respectively by the Supreme Allied Commander Europe (SACEUR) and the Supreme Allied Commander, Transformation (SACT).

NATO Organization Structure List

EXERCISES

The primary role of Alliance military forces is to protect peace and to guarantee the territorial integrity, political independence and security of the member states. Alliance forces must be able to deter and defend effectively. The Alliance remains subject to a wide variety of military and non-military risks that are multi-directional and often difficult to predict.

List of current NATO Exercises

The term NATO Military Exercise includes all exercises for which NATO is the initiating or the joint initiating authority. Associated with NATO Military Exercises are building blocks, such as: seminars, study periods and workshops.

### 2NC – AT: PDCP – AT: Member States

#### The plan must engage via NATO’s independent international legal personality---that’s distinct from NATO’s member states

Frans A. Nelissen 11, T.M.C. Asser Institute, “The Relationship Between International Organisations and Their Member States - Who Pays the Check?,” Evolving Principles of International Law: Studies in Honour of Karel C. Wellens, Martinus Nijhoff Publishers, 11/11/2011, Google Books

2.3.3. NATO Actions in Yugoslavia

A controversial topic with regard to the responsibility of international organisations is the attack carried out by NATO on Yugoslavia. As is well established, NATO is an international legal personality capable of engaging in international relations. The military operation was carried out based on a decision of the North Atlantic Council, the political governing body of NATO. When it became clear that during the bombardments damages were inflicted on other than military targets on Yugoslavian territory, NATO paid compensation to individuals whose properties were damaged. Clearly, the member states did never consent to the execution of those failed missions. Nevertheless, Yugo-Slavia decided to bring claims against the NATO members separately, and not NATO itself, before the European Court of Human Rights (ECHR) and the International Court of Justice. NATO is neither a party to the ICJ Statute nor to the ECHR, so there was no other alternative. This implied that the NATO cover of the missions had to be lifted in order to effectively bring a complaint. During the proceedings, the NATO members surprisingly did not bring forth the argument that it was the NATO carrying out the attacks and not the member states, and that the member states could rely on the liability of the alliance. Therefore, neither the ICJ nor the ECHR had to deal with the issue during those proceedings. NATO has the capacity to Carry out military attacks such as those in Yugoslavia, but was in casu not called upon to answer for the incurred damages. On the other hand, a decision of the North Atlantic Council is an authoritative instrument, and states should be able to rely on its legitimacy when carrying out the decision as long as they remain within the mandate given.

#### The difference is vital and fundamental

Brian Collins 2, Lt. Col. In the US Air Force and a faculty member of the National War College in Washington, D.C., “Operation Enduring Freedom and the Future of NATO,” Georgetown Journal of International Affairs, vol. 3, no. 2, Georgetown University Press, 2002, pp. 51–56

The U.S. -led military action in Afghanistan in response to the attacks of September II raised a number of important issues regarding the future of the North Atlantic Treaty Organization (NATO) and the relationship between the United States and its transatlantic allies. On September 12, , NATO invoked Arti- cle 5 - the mutual defense clause of the Washington Treaty - thereby committing NATO to help defend the United States from the perpetrators of the attacks. Shortly thereafter, NATO sent seven of its Airborne Early Warning and Control (AWACS) aircraft, crews, and ground support personnel to assist in the air defense of the United States. In addition to demonstrating NATO's military resolve and buttressing the political declaration of Article 5» the deployment of NATO AWACS aircraft also freed up U.S. aircraft for Operation Enduring Freedom in Afghanistan.

NATO also provided blanket air rights for U.S. aircraft, access to bases and ports, and other non-combat support. However, NATO did not lead Operation Enduring Freedom, nor did it develop the International Security Assistance Force (ISAF) deployed to Afghanistan in the wake of the American rout of the Taliban. The Europeans expected more of a say in the planning and execution of operations since the alliance had stood firm with the United States after the attacks. Since the understanding for fifty years had been that the United States would come to the aid of Europe and lead its defense, it was only natural to assume that Europe would play a large role if the United States was attacked. However, this was not the case; the United States preferred a coalition involving NATO members but not NATO itself.

European members of NATO asked whether this American unilateralism portended the end of the alliance. Americans vigorously denied this, and argued for a broader conception of NATO. Nevertheless, Operation Enduring Freedom was a landmark event because the United States chose to use a loose coalition instead of the NATO alliance, a decision that revealed an emerging U.S. -NATO relationship in which the United States consults with NATO on security issues but acts outside the alliance structure when it is in America's interest.

Why the United States Didn't Turn to NATO. In the aftermath of September II, the United States wanted the form of a coalition, but not the sub- stance, for several reasons. First, the attacks were on American soil, and consequently the United States had to lead the response. Although citizens from scores of countries were killed in the attacks, it was clear that the United States, its people and its homeland, was the intended victim. Therefore, a response to the terrorist attacks did not automatically involve NATO. Ultimately, there was no direct link to Europe. Consulting NATO would have been unrealistic, and no American administration would have waited for NATO to form a response.

NATO was also not the United States's first choice because there is no clear consensus on how to interpret the Washington Treaty in the post-Cold War world. For example, although the treaty does not place explicit restrictions on NATO operations in a geographical sense or require United Nations approval for its operations, many members have conceptual difficulty expanding NATO's role beyond the alliance's immediate periphery, especially in the absence of UN man- dates for such operations. Consequently, rather than get embroiled in discussions regarding the legality of NATO participation in Afghanistan, the United States sidestepped the issue and worked with its allies outside of official NATO channels.

### 2NC – AT: PDCP – AT: Member States – Security Assistance

#### That distinction extends to security assistance

Gary Mead 22, “Soapbox: Who will pay?,” GLINT - The Global Currency, 4-12-2022, https://glintpay.com/en\_us/blog/soapbox-who-will-pay/

Proxy war, proxy money

One of the terrors that Moscow has already dangled in the face of the West is an escalation of the Ukraine conflict. Putin has put his nuclear forces on high alert, a Sword of Damocles hanging over Brussels and Washington D.C. NATO members – crucially not NATO itself – are supplying Ukraine with weapons, such as the tanks, rocket launchers and artillery that have been sent from the Czech Republic. NATO is thus fighting a proxy war with Russia.

## To Cut

### 2NC – hunt forward

<https://breakingdefense.com/2021/11/cybercoms-no-2-discusses-hunt-forward-space-cybersecurity-china/>

https://www.960cyber.afrc.af.mil/News/Article-Display/Article/2433491/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/

### 2NC – S – SFKSDLF

#### Bilat solve

Pernik, '21 – Piret Pernik is a researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). She has researched cybersecurity strategic and policy aspects since 2013. She has published research reports and analyses on cyber resilience, military 5G security, cyber commands, and cyber defence training (Piret Pernik; "Cyber deterrence: A case study on Estonia’s policies and practice"; Hybrid CoE; https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012\_Hybrid\_CoE\_Paper\_8\_Cyber\_deterrence\_WEB.pdf; 10-2021, Accessed 6-27-2022)//ILake-NoC

Credible cyber deterrence was associated with international cybersecurity cooperation and Estonia’s efforts to strengthen international cyberspace stability. In this respect, this document communicated a view of the Estonian Foreign Policy Development Plan 2030, but provided more details. For example, hosting international cybersecurity events and cyber exercises in Estonia, establishing NATO-associated facilities (such as NATO’s cyber range and NATO CCDCOE located in Tallinn) and other allied infrastructure in the country are considered important for fostering credible deterrence. In like manner, binding agreements with key allies and regular cyber defence exercises and training sessions are seen as mechanisms for implementing cyber deterrence in practice.84 Notably, Estonia has bilateral cybersecurity and cyber defence agreements with several NATO allies (the US and France), and has established a joint platform for secure cyber threat intelligence-sharing with the US. Thus, operational-level and technical bi- and multilateral cooperation, including information- and intelligence-sharing and technical exercises, are viewed as critical components of strategic deterrence against cyberattacks.85 This reflects a pragmatic understanding that high-level political declarations and commitment cannot deter cyberattacks, but timely cyber threat intelligence can.

In accordance with the strategy, a necessary element of deterrence is an ability to attribute cyberattacks. The strategy prescribes developing a procedure to attribute attacks, which includes political, legal and technical criteria (this mechanism 23 was established in 2019) and measures to attribute cyberattacks in the grey zone (below the threshold of armed attack). Estonia must actively attribute attacks together with partners and implement collective countermeasures.8

#### bilat

Inserra, '17 – Former Policy Analyst for Homeland Security and Cyber Policy (David Inserra; "Cybersecurity Beyond U.S. Borders: Engaging Allies and Deterring Aggressors in Cyberspace"; Heritage Foundation; https://www.heritage.org/cybersecurity/report/cybersecurity-beyond-us-borders-engaging-allies-and-deterring-aggressors; 7-14-2017, Accessed 6-27-2022)//ILake-NoC

Greater Collaboration with Allies and Partners. In addition to combatting cybercrime, nations must also work together to decrease their vulnerability to attack and reduce the consequences of a successful attack. Collaboration on cybersecurity defenses, technology, organizations, training, and exercises across both military and civilian portions of the network is an essential step toward cybersecurity. While no defense is perfect in cyberspace, more can be done to improve upon the status quo.

On the civilian side, constant and regular engagement among U.S. and foreign Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) is a necessity.29

Such engagement must not only occur when there is a cyber incident, but must take place regularly to ensure that all sides know their counterparts and have developed formal as well as informal relationships. This requires that the U.S. and partner CERTs/CSRITs have the resources to deal not only with the technical and information-sharing aspects of cybersecurity, but also to build relationships with cybersecurity experts in other countries. The U.S. should encourage allies to expand cyber capabilities and expand cross-border training and exercises to prepare for cyber incidents.

Beyond the response aspects, the U.S. must also seek greater cooperation with allies on cybersecurity policies and strategies. While improved technical capabilities, trust, and relationships between those in the trenches on cybersecurity are critically important, policymakers and strategists are necessary to ensure that such capabilities and relationships are advancing U.S. and allied interests and objectives. The Russians and Chinese have each developed their own ways of integrating cyber weapons and tools into their hybrid or information warfare strategies. Indeed, they do not just have strategies on paper, but are putting them to work in Ukraine, the U.S. political arena, the South China Sea, and elsewhere.

The U.S. must have a fully formed cyber strategy that includes both civilian and military components. U.S. military planners and their international partners must consider how allied forces will fight in cyberspace. In 2016, NATO declared cyberspace to be a domain of warfare in the same way that the air or the seas are.30

Such a declaration is overdue, and preparations to fight in this domain must now play catch up. NATO members and other allies must make investments in cyber capabilities that will protect and advance military objectives, in addition to much-needed investments in traditional tools of warfare. The U.S. should push for expanded partner preparation and capabilities in the domain, offering assistance where it can. Similarly, training in cyberspace and hybrid conflicts are necessary to enable the U.S. and allies to be prepared for future conflicts.

Furthermore, policymakers need to devise ways of ensuring that the private sector is also playing a leading role in cybersecurity. Government-to-government cooperation on cybersecurity must ultimately be built on private-sector expertise and control. In many countries, including the U.S., critical infrastructure is primarily owned and operated by the private sector. Even in countries where this is not true, the private sector still provides the vast majority of the goods and services, faces countless cyber attacks, and serves as the greatest repository of expertise on cybersecurity. So, any government policies on cybersecurity require true partnership with, and reliance on, the private sector. This reality should not be lost in efforts to increase cooperation between governments but should inform the way policy cooperation occurs.

Responding to Cyber Aggression

While there is much the U.S. can and should do to defend against cyber aggression both independently and in conjunction with allies and partners, the U.S. should also go beyond just defending its systems. Given the nature of cyberspace as described earlier, defense will not always succeed. When faced with an offensive-dominated domain, the U.S. can instead seek to raise the costs of hacking through various types of retaliation. These forms of retaliation should be viewed as a toolbox that can be used and tweaked depending on the aggressor to which the U.S. is responding.

### 2NC – S – Info sharing

#### YES

O’Mahony et al., '22 – associate dean for academic affairs at Pardee RAND Graduate School and a senior political scientist at RAND (O'Mahony, Angela, David E. Thaler, Beth Grill, Jennifer D. P. Moroney, Jason H. Campbell, Rachel Tecott, and Mary Kate Adgie; "Prioritizing Security Cooperation with Highly Capable U.S. Allies: Framing Army-to-Army Partnerships"; RAND Corporation; https://www.rand.org/content/dam/rand/pubs/research\_reports/RRA600/RRA641-1/RAND\_RRA641-1.pdf; 2022, Accessed 6-27-2022)//ILake-NoC

As the Army prepares for the possibility of near-peer conflict and focuses on increasing its expeditionary agility, developing and maintaining the ability to interoperate quickly and effectively with highly capable allies will become increasingly important. A key reason that U.S., British, and Australian personnel have been able to work together so well in recent operations is the steady state interactions between these allies, ranging from high-level embeds, multinational exercises (e.g., joint warfighter exercises), education and training programs,10 and officer and unit exchange programs (e.g., the Military Personnel Exchange Program). However, the British Army explicitly states that the integration skills jointly developed during nearly five years in Afghanistan are perishable and that a comprehensive defense engagement program to preserve these lessons should be developed: “The challenge during this fallow period before the next coalition operation is how to start the next operation as an integrated coalition, capitalising [sic] on those coalition synergies from the start.”11

Implications

Given the relative dearth of SC activities during ongoing operations, the low likelihood that these will become more common in future operations, and the importance of steady-state SC activities for preparing units and personnel to work together rapidly and effectively in the absence of predeployment training, we identified the following implications:

• Steady state SC activities between the United States and highly capable allies should continue to focus on providing opportunities for developing and exercising operational partnering. As discussed, such efforts are a central aspect of security relationships between the United States and its closest partners. These activities should emphasize not only developing soldiers’ skills and familiarity but also developing procedures for shared communications, processes, and logistics. Waiting until an operation occurs is too late to develop operational partnerships.

• Mission-essential tasks related to multinational interoperability should be considered for steady-state U.S. unit training to enable swift, effective operational partnering. For units that engage in multinational training, incorporating interoperability and operational partnering into unit mission-essential task lists could help ensure that the appropriate activities are highlighted in exercises with highly capable allies that prepare them to work together not only in near-peer conflicts, but also contingency operations in other contexts.12

United States and Allies Share Information, But Only Opportunistically

At a basic level, most SC is about sharing information. Although most information sharing through SC occurs outside ongoing operations, we analyzed activities that were designed to share lessons with highly capable partners during operations in Iraq and Afghanistan. As with predeployment training, formally organized cooperative activities to share operationally relevant lessons were rare. That said, throughout our research, we sought examples that demonstrated how valuable it was for U.S., British, and Australian forces to share operational lessons with each other. A few representative examples stand out.

As previously mentioned, the United States and United Kingdom occupied a shared battlespace in Afghanistan’s Regional Command Southwest and integrated their air and targeting efforts to prevent seams and help optimize support for ground forces. At a more micro level, U.S. and British personnel consistently shared lessons learned and incorporated them into their evolving TTPs. For instance, a procedure routinely used by Royal Navy pilots that was seen as good operational practice was adopted by the rest of the United Kingdom’s Joint Aviation Group as well as the U.S. Marine Corps’ Air Combat Element, which extended to briefing formats and general mission business.13 U.S. Marines deployed to Regional Command Southwest credited the United Kingdom with helping them refine their targeting practices, particularly how best to use the varying capabilities of multiple intelligence, surveillance, and reconnaissance platforms tasked with tracking one or a group of potential targets.14

Given that distribution of lessons learned within the Army—much less at the joint and combined force levels—is highly problematic,15 these types of information-sharing activities tended to emerge organically rather than as part of an institutionalized sharing process. When we followed up with operators on how lessons tended to be shared, we were told that information sharing generally occurred through three pathways. First, personnel found themselves in the same place at the same time and informally discussed their operational experiences with each other—that is, they “talked shop.” Second, if personnel were aware of each other’s operations, they might reach out for insights in the face of current challenges. Third, embedded partner personnel would act as formal or informal liaisons to share lessons with personnel from both countries. Operators noted that sharing lessons was helpful, but it generally only occurred opportunistically. This raises the concern that fewer lessons are shared with allies than is optimal during operations.

On the other hand, the Combined Joint Task Force in OIR experienced severe difficulty formally sharing information among coalition partners, largely because of differing communication systems and problems with classification. It was not until the joint operations center began to use Global Command and Control System–Joint that coalition personnel could fully see the required common operational picture needed for the operation. An insight reported by the Center for Army Lessons Learned suggested that plans for information sharing across the coalition should be in place before an operation starts.16

When we asked interview respondents about potential shortcomings in operationally relevant information sharing, many thought that developing a mechanism for sharing operationally relevant observations across coalition partners would be useful—particularly if these mechanisms were made available to units prior to deployment.

Implications

Documenting lessons learned and sharing information between different offices and across time is a perennial challenge for the Army. Our first two implications focus on enabling bottom-up communications between units undertaking similar missions of operating in similar environments. The third and fourth focus on shared communications infrastructure:

• Develop updated guidance for deployed U.S. units on lessons learned for communications with allied units. Communications sometimes happen naturally in an operational setting. However, the Army could formalize guidance to deployed units on identifying allied counterpart units that have conducted or are conducting similar operations in the combined battlespace and initiating interactions designed to share experiences. Such exchanges could help each unit address challenges that have arisen during operations.

• In instances in which the United States and an ally have developed clear interoperability workarounds in the field, ensure that they are incorporated into interoperability plans and roadmaps. Successful workarounds are important to capture and archive for use in future operations and exercises with the ally; they could also be improved and expanded to include other allies.

• Formal, pre-established information-sharing mechanisms should be in place to increase lines of communication on combined lessons learned during operations. DoD efforts toward establishing and exercising mission partner environments can serve as the foundation for a shared communications network.17

• Capturing allied lessons learned would be useful as part of the Joint Lessons Learned Information System. Building a separate allies and partners lessons learned information system might be unnecessary; including such a lessons learned portal as part of an operational communications infrastructure might be useful. Within this portal, providing a template for contributing observations and a list of common topics for tagging observations would increase the value of captured data.

### 2NC – S – Coordination

#### SDSD

O’Mahony et al., '22 – associate dean for academic affairs at Pardee RAND Graduate School and a senior political scientist at RAND (O'Mahony, Angela, David E. Thaler, Beth Grill, Jennifer D. P. Moroney, Jason H. Campbell, Rachel Tecott, and Mary Kate Adgie; "Prioritizing Security Cooperation with Highly Capable U.S. Allies: Framing Army-to-Army Partnerships"; RAND Corporation; https://www.rand.org/content/dam/rand/pubs/research\_reports/RRA600/RRA641-1/RAND\_RRA641-1.pdf; 2022, Accessed 6-27-2022)//ILake-NoC

Engagement Partnering for Future Shaping

Both the United States and its key allies also engage in SC with third countries to pursue strategic interests focused on long-term competition. The objectives for these activities tend to be (1) building partner capacity to shape and maintain regional stability or to prepare for possible operations, (2) increasing access or influence in key geographic areas, and (3) improving U.S. and allied strategic competitiveness vis-à-vis other global actors. Most SC engagements with third parties occur bilaterally, but in recent years initiatives have been undertaken to coordinate allied efforts.

Building Partner Capacity for Future Operations

The United States and its European allies have placed greater emphasis on building partner capacity for engaging in conventional military operations since 2014. U.S. Section 333 SC capacity-building projects in the U.S. European Command have increasingly been targeted at the Eastern European flank. Germany, the United Kingdom, and Canada have also increased their contributions to partnership capacity building through their leadership of Enhanced Forward Presence battlegroups in Lithuania, Estonia, and Latvia, respectively.27 Other efforts include TACET, which was created by Germany and the United States to synchronize military training and exercises in the Baltic states and Poland, and the Combined Joint Enhanced Training Initiative, which provides coordinated training in Bulgaria and Romania.28 These initiatives have evolved into other efforts, such as the Capability Enhancement Regional Symposium, a multilateral forum in which NATO allies and key partners share regional situational awareness and visibility on their bilateral activities with the Baltic states and Poland. The Capability Enhancement Regional Symposium has been focused on evolving threats, such as multidomain awareness and cyber security.29

U.S. capacity-building efforts in the Pacific region are growing as well, with dedicated funding toward building ally and partner maritime security capabilities. The Philippines, Vietnam, Indonesia, and Malaysia are examples of participants in the South East Asia Maritime Security Initiative. The Army’s Pacific Pathways program has included bilateral (and some multinational) exercises with Indonesia, Japan, Korea, Malaysia, Philippines, Singapore, and Thailand to build partner capacity.30

These efforts were strengthened by coordinated regional engagements with Australia, Japan, and South Korea to build maritime security and domain awareness in the region. As with the United States, many of the partner capacity-building efforts undertaken by Australia and other highly capable allies are conducted on a bilateral basis. Examples include engagements by the Australian Defence Force to train the Armed Forces of the Philippines on countering complex urban terrorist tactics and maritime training initiative.