CSIS BRIEFS

Battle Networks and the Future Force

Part 3: The Role of Allies and Partners

By Todd Harrison and Christopher Reid

MARCH 2022

THE ISSUE

This CSIS brief is the third in a series on the future of battle networks and Joint All-Domain Command and Control (JADC2). The **first brief** *in the series examined the importance of battle networks to modern military operations and presented a framework of five functional elements that make up a battle network. The* **second brief** *used lessons learned from previous attempts to improve battle network integration to explore how the Department of Defense (DoD) can properly scope the problem it is trying to solve and organize itself to effectively and efficiently acquire the systems needed to realize its vision for JADC2. This brief focuses on the importance of integrating allies and partners into future battle networks, particularly in the Indo-Pacific region. It explores existing agreements, opportunities for new agreements, and the technical and policy challenges for battle network integration across allied and partner nations. It concludes with an assessment of how combined battle networks with allies and partners can serve as the key enabling technology toward a new offset strategy.*

EXISTING AGREEMENTS AND COMBINED BATTLE NETWORKS

While the speed and scope of battle networks has increased significantly in recent decades, the value of integrated battle networks and information sharing with allies and partners has long been understood. In the years leading up to World War II and throughout the war, the United States formed close intelligence-sharing agreements with allied nations. The United States and United Kingdom reached a formal agreement in 1942 to collaborate and streamline technical collection and analysis of signals intelligence on Japan, Germany, and Italy—a collaboration that the Congressional Research Service **concluded** "proved pivotal in the Allies establishing information dominance during the war."

In 1946, the United States and United Kingdom created a broader intelligence-sharing agreement that evolved to include Canada, Australia, and New Zealand—what is now known as the Five Eyes agreement. It is arguably the most extensive data-sharing and collaboration agreement for the U.S. military and intelligence community (IC) today, and the U.S. military's internal security policies are built to support access and collaboration with Five Eyes partners above all others. The level and frequency of data sharing has also **evolved over time** to include both tactical and strategic intelligence and real-time data transmission through interoperable battle networks.

The creation of the North Atlantic Treaty Organization (NATO) in 1949 led to an expansion of bilateral and multilateral military agreements, many of which enabled greater data sharing and battle network integration. These agreements have evolved over time, and NATO has made substantial progress in developing common data standards to enable a higher degree of interoperability across member nation forces and platforms. At the 2012 Chicago Summit, NATO leaders **agreed to a set of goals**, known as NATO Forces 2020, to create "modern, tightly connected

forces equipped, trained, exercised and commanded so that they can operate together and with partners in any environment." One of the efforts that resulted from this was the Connected Forces Initiative that is specifically intended to increase the level of interoperability and connectivity among member nations.

NATO data standards and data-sharing agreements proved invaluable in creating the basis for combined battle networks for coalition operations in Afghanistan. NATO implemented the Afghanistan Mission Network in 2010 that integrated multiple national and NATO networks into a single combined battle network. As a **previous RAND report** notes, the Afghanistan Mission Network shifted the coalition information-sharing posture from "need to know" to "need to share." Based on the success of this effort, NATO institutionalized the approach in the **Federated Mission Networking** framework and governance structure **beginning in 2012**.

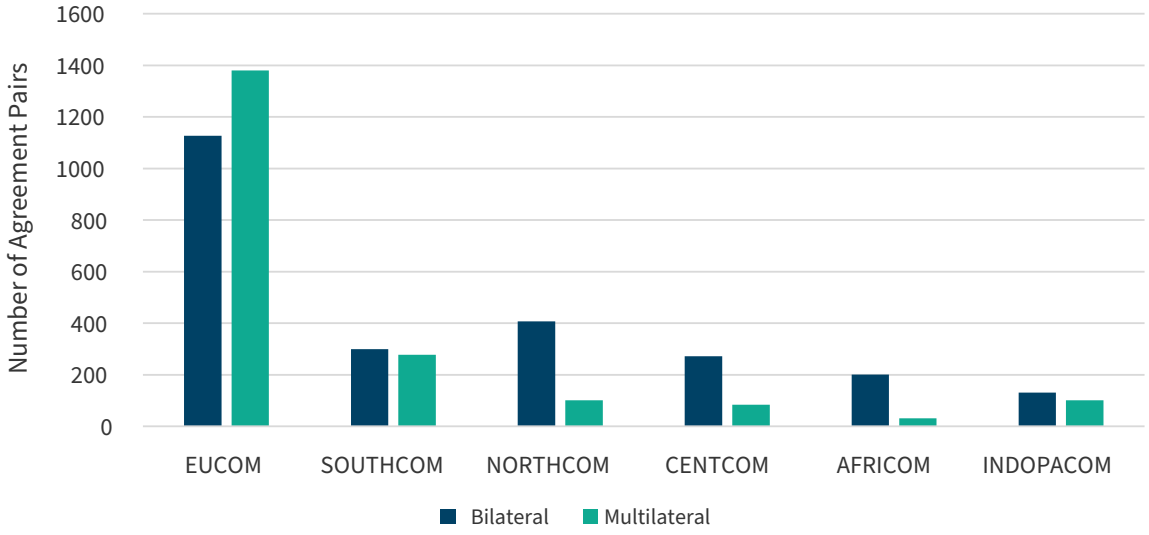
The **Partnership Interoperability Initiative** (PII), launched during the 2014 Wales Summit, was designed to enhance interoperability investments beyond NATO member nations, often through exercises and dialogue with key NATO partners. As part of PII, NATO launched the Interoperability Platform "to provide a wider group of partners with deeper access to cooperation on interoperability issues." The alliance now counts 23 partners as part of this program, and these partners can participate in meetings of relevant NATO committees to deepen interoperability in preparation for future contingencies. Shortly after this effort began, the **Enhanced Opportunities Partners** (EOP) framework agreement was established with Australia, Finland, Georgia, Jordan, and Sweden (**and Ukraine in 2020**) to develop more familiarity among forces and to enhance "**access to interoperability programs and exercises."** The EOP framework provides opportunities for future intelligence sharing and improved indications and warnings for the complex manifestations of aggression the world faces today, including hybrid warfare and gray zone conflict. While inclusion as a NATO partner under PII or EOP is not predicated on adhering to NATO's military data standards, deeper participation in exercises and the desire for stronger military integration provide strong incentives for partner nations to move in this direction.

UNDERSTANDING THE BREADTH AND VALUE OF U.S. ALLIES AND PARTNERS

Lessons learned from operations in Afghanistan, Iraq, and Syria made clear that coalition warfare—particularly the ability to integrate forces and share data seamlessly on the battlefield—provides a significant and enduring strategic advantage. The **Interim National Security Strategic Guidance,** issued by the Biden administration in 2021, reinforces the importance of allies and partners, noting that the United States has an "unmatched network of alliances and partnerships." Moreover, the **Indo-Pacific Strategy**, released in February 2022, states that the United States' "single greatest asymmetric strength" in the Indo-Pacific region is "our network of security alliances and partnerships."

A **2014 analysis** by Jennifer Kavanagh at RAND examined more than 5,500 security-related agreements between the United States and other nations. These included bilateral and multilateral agreements with virtually every nation around the world, including allies, partners, and

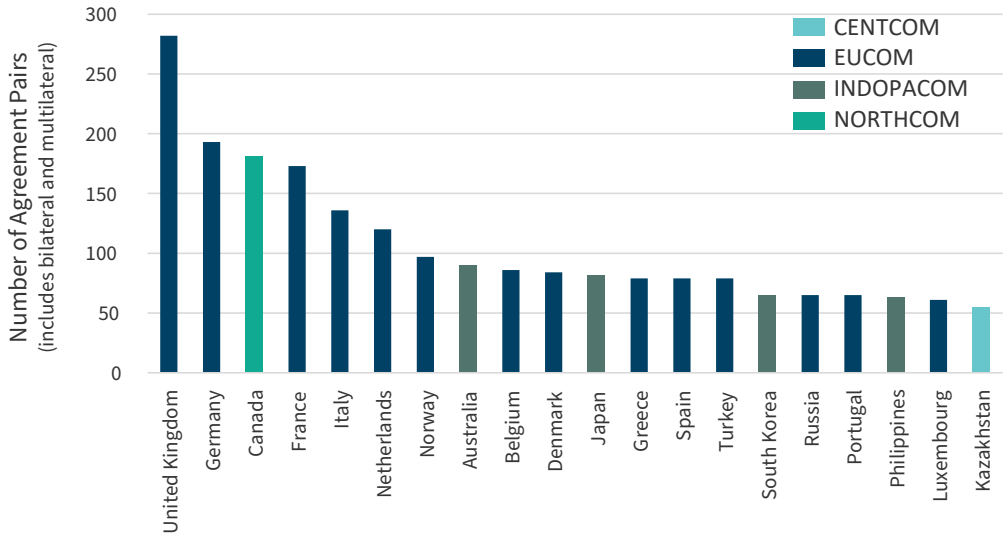
Figure 1: Number of Military Agreements by Geographic Region, Current as of 2012



Source: Jennifer Kavanagh, U.S. Security-Related *Agreements in Force Since 1955: Introducing a New Database* (Santa Monica, CA: RAND, 2014), https://www.rand.org/pubs/research_reports/RR736.html (updated by authors to reflect current COCOM AORs).

adversaries. In total, 4,414 of these agreements remained in effect through 2012. Despite the broad range of nations included, these security-related agreements were not evenly distributed across the geographic combatant command (COCOM) areas of responsibility (AOR). Of the agreements still in effect as of 2012, the largest number of bilateral and multilateral agreements (46 percent and 70 percent, respectively) are with nations that fall within the European Command AOR, as shown in Figure 1, which was updated to reflect the current COCOM AOR assignments of nations. This largely reflects the United States' focus throughout the Cold War on Europe, and NATO-related agreements alone make up 550 (or 40 percent) of the EUCOM multilateral agreements shown in the data. Figure 2 lists the top 20 nations by the total number of security agreements with the United States. Of these, 14 nations are part of EUCOM, while only 4 are part of INDOPACOM. Within the INDOPACOM AOR, nearly 60 percent of U.S. security-related agreements are with Australia, Japan, South Korea, and the Philippines, as shown in Figure 2.

Figure 2: Number of Military Agreements by Nation, Current as of 2012



Source: Kavanagh, *U.S. Security-Related Agreements in Force Since 1955*.

The number of security agreements alone does not fully convey the depth of cooperation between the United States and each of its allies and partners, but the variety of nations included demonstrates the broad reach of U.S. alliances and partnerships around the world. Some of the agreements included in this comprehensive data set are for other types of military cooperation or coordination beyond data sharing and interoperability—to include agreements between the United States and Russia, China, and Cuba, to name a few notable examples. But this data demonstrates that the historical focus of the United States on Europe and NATO—reflected in the number of agreements in this region—created the opportunity for deeper military-to-military integration. As previously discussed, a tangible result of the various NATO-related agreements is the creation of common NATO data standards for interoperability as well as partnership programs and technical frameworks designed to integrate battle networks for combined military operations. The United States' strong network of allies and partners creates the potential for unmatched military advantage, but this advantage cannot be fully realized unless allied and partner forces are able to operate together in a coherent and coordinated manner through combined battle networks.

OPPORTUNITIES FOR NEW, REVISED, OR EXPANDED AGREEMENTS

The shift in strategic focus away from counterinsurgency, counterterrorism, and nation building toward a long-term competition with China and Russia, as articulated in successive **defense strategies** and **strategic guidance** since 2012, requires new, revised, and expanded agreements that specifically enable the kinds of real-time data sharing necessary for combined battle network integration—particularly in the Indo-Pacific region. The Indo-Pacific strategy calls on the United States to "work with allies and partners to deepen our interoperability and develop and deploy advanced warfighting capabilities." Current JADC2 efforts, however, are mainly focused on achieving basic interoperability among the U.S. military services and are just beginning to consider integration with allies and partners. For example, the Army's flagship JADC2 program, Project Convergence, is planning to **include some of the Five Eyes partners** in its 2022 exercises and experiments, while the Air Force's Advanced Battle Management System (ABMS) program is only **focused on connecting U.S. Air Force aircraft** in its first capability release.

The strategic focus on countering China and bolstering deterrence in the Indo-Pacific region requires data sharing and battle network integration agreements beyond the existing Five Eyes and NATO constructs. A key strategic priority should therefore be expanding agreements with Japan and Korea and establishing a broader multilateral framework agreement for the Indo-Pacific region, potentially among the Quadrilateral Security Dialogue (Quad) nations.

An eight-ship joint-coalition formation flies over Guam during exercise Cope North 21, near Andersen Air Force Base, Feb. 9, 2021.

Photo credit: Staff Sgt. Divine Cox

While formally adding nations to the Five Eyes agreement may be difficult, there is growing support for expanding agreements beyond the Five Eyes and specifically in the Indo-Pacific region. In a **statement** accompanying the Intelligence Authorization Act for FY 2020, FY 2019, and FY 2018, the House Intelligence Committee noted that intelligence sharing and cooperation is less robust for non-Five Eyes partners. The committee specifically expressed support for "the roles and contributions of third-party partners such as India, Japan, and South Korea, and recognizes their ongoing contribution toward maintaining peace and stability in the Indo-Pacific region."

As noted in a recent **CSIS paper**, Japan has worked diligently in recent years to prepare for greater intelligence sharing and military integration with key allies beyond just the United States. In 2020, Japanese defense minister Taro Kono reiterated Japan's interest in developing a closer intelligence-sharing partnership with the United States and its Five Eyes partners. He was **quoted as saying**, "These countries share the same values. Japan can get closer [to the alliance] even to the extent of it being called the 'Six Eyes.'" The defense minister argued that Japan offers a geo-intelligence network centered in the Indo-Pacific region that can fill in many gaps in the intelligence networks of existing NATO and Five Eyes nations. Japan is also particularly adept at technical collection, such as signals intelligence (SIGINT). In 2020, Japan expanded the scope of its state secrets law to include information sharing with other nations, but these efforts may be insufficient to assure existing Five Eyes nations. For example, under its **current policy**, "all government staff, subcontractors, and prefectural police officers can view classified information, provided they aren't deemed to be a security risk," and Japan does not yet have comparable security levels and compartments for limiting access to classified information.

Other analysts cite the importance of including South Korea in intelligence-sharing agreements. **Kathyrn Botto** writes that "trilateral cooperation is more than a force multiplier—it is integral to ensuring the United States, South Korea, and Japan can prevent catastrophic conflict, loss of life, and widespread destruction on all sides." However, she notes that differences between South Korea and Japan in terms of their military aims, how they approach both North Korea and China, and how Japan should amend for its colonial past have proven to be a barrier to greater military and intelligence cooperation. While bilateral relations between South Korea and Japan have been strained in recent years, this underscores the need for expanded multilateral cooperation with the United States and other allies that can help buffer and transcend regional and historical differences.

One such multilateral framework that could be the basis for increased cooperation and data sharing is the Quad, which includes the United States, Australia, Japan, and India, and the Quad Plus group of nations, which adds New Zealand, South Korea, and Vietnam. What unites the Quad nations is the **shared belief** that the Indo-Pacific region should be "free, open,

inclusive, healthy, anchored by democratic values, and unconstrained by coercion." The Quad and Quad Plus are not formal alliances but are instead based on functional cooperation for mutually beneficial purposes. This cooperation can serve as an important balance against China's growing power and influence in the region, and the alignment of shared interests could serve as the foundation for broader data- and intelligence-sharing agreements and interoperability.

TECHNICAL AND POLICY CHALLENGES

As a **Congressional Research Service report** notes, "non-Five Eyes allies have occasionally expressed frustration with bilateral intelligence ties that are evidently not as close as those of each of the Five Eye countries to the United States." The report finds that the barriers to greater collaboration and data sharing can be attributed to a combination of factors: (1) intelligence agreements that are insufficient or place too many restrictions on what can be disclosed; (2) differences in privacy protection laws among allied and partner nations; (3) differences in fundamental values (e.g., respect for human rights); (4) different perceptions of the threat environment; and (5) nations using intelligence sharing as leverage to gain benefits in other areas (e.g., access to technology, weapons, and financial support).

Beyond the Five Eyes nations, NATO has championed the concept of federated interoperability as a framework for overcoming some of these barriers. NATO **defines** federated interoperability as a collective effort "to act together coherently, effectively and efficiently to achieve Allied objectives." Rather than top-down directives or standards for how partner nations design and build their battle networks, the alliance accepts that individual nations will inherently have heterogeneous battle networks but also that the overall architecture should be open to networking and data sharing across nations.

A federated interoperability approach can similarly be applied to other regions and with allies and partners beyond NATO. The goal of federated interoperability is not to give each nation access to all data from all partners at all times. Rather, the goal is to get the right data to the right coalition forces at the right time. But doing that requires overcoming several technical and policy challenges, including integrating across dissimilar platforms, translating across data standards and formats, and navigating different levels of security and data releasability.

The goal of federated interoperability is not to give each nation access to all data from all partners at all times. Rather, the goal is to get the right data to the right coalition forces at the right time.

INTEGRATING ACROSS DISSIMILAR PLATFORMS

One of the main technical challenges to integrating battle networks with allies and partners is the use of different platforms and weapon systems. However, this is not a unique challenge to allied and partner integration, because the U.S. military faces similar internal issues integrating across legacy, current, and future platforms within its own forces. Allies and partners bring a greater diversity of equipment, some of which may pose unique challenges for integration. The task is made easier when nations are using many of the same platforms. For example, **13 nations** (other than the United States) are currently planning to buy the F-35, including the key Indo-Pacific nations of Australia, Japan, Singapore, and South Korea. The F-35 uses common mission software, communications links, and sensor suites across all variants of the aircraft for all partner nations, virtually eliminating many of the **technical obstacles** to data sharing.

Dissimilar platforms can be integrated to share data by using common communication links or connecting through communication hubs. For example, NATO uses **Link 16** for tactical data links, and more than 5,000 different platform types across the alliance incorporate Link 16 into their communications capabilities. Widespread adoption of common data links greatly enhances interoperability, but some platforms and missions may require **tailored or unique data links**. It also may not be cost feasible to upgrade some legacy platforms to include common data links such as Link 16. In these instances, the best alternative may be to create communications hubs or **teleports** that house a variety of different communications systems and can connect across any number of them. These communications hubs can be at fixed ground sites, on **airborne platforms**, or in **space**. The risk with using hubs or teleports is that these nodes in the network become attractive targets for an adversary because taking out one of them could have outsized effects on the overall functionality of the battle networks it supports. Communications nodes must therefore be designed for resilience.

TRANSLATING DATA STANDARDS AND FORMATS

The fact that platforms and weapons can pass data through interoperable communication links does not necessarily mean they can use the data they are sharing. Different sensors and data processing systems may use different data standards and formats, which can limit the ability to translate information across dissimilar systems. The ideal approach to simplify interfaces would be to develop and use common data standards and formats across platforms and nations. While this may work for some future systems, it does not address the large number of existing systems already fielded in allied and partner forces.

One approach to sharing data across dissimilar standards and formats is to create middleware that translates between them. This middleware would need to be custom adapted to each unique data system that needs to connect in a network. The Defense Advanced Research Projects Agency (DARPA) developed a tool that can speed the creation of such middleware as part of the System-of-systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (**STITCHES**) program. The advantage of this approach is it does not require hardware or software changes to existing systems, but the middleware must be configured in advance and can take several days for each unique set of equipment.

NAVIGATING SECURITY LEVELS AND DATA RELEASABILITY

Another challenge to sharing data across allied and partner battle networks is the various security levels of the data involved. Data security is both a technical and policy issue that each of the nations involved must coordinate in advance. But as the coalition of nations in Afghanistan learned, navigating security levels and data releasability requires a shift in mindset from "need to know" to "need to share." Battle networks commonly use data at multiple levels of security. In many cases today, this results in separate systems being used in parallel at each level of classification, and data is passed across levels using manual processes that are slow and subject to error. Sharing classified data with allies and partners is further complicated by the need for transparency and confidence in the encryption, data systems, access controls, and physical security being used by other nations. The use of **commercial systems** for intelligence, surveillance, and reconnaissance collection and dissemination can be a useful way to sidestep security issues because this data is unclassified and fully releasable.

Many of these security issues ultimately need to be handled at the policy level. Nations need to agree on encryption methods and certification processes to be confident that data will be transmitted and stored securely. They also need to agree on how facilities and personnel are vetted to have access to data at different levels of classification. Policy agreements may also need to address supply chain issues and the vetting of parts and components to be used in sensitive data systems. As a **recently published CSIS report notes**, many of these policy issues intersect with the activities, legacy systems, and networks managed by the Defense Information Systems Agency (DISA). Yet, despite its massive portfolio for globally accessible information infrastructure (including support to allies and partners), DISA's role and relationships with the joint staff and military departments in JADC2 development is not well defined.

COMBINED BATTLE NETWORKS AS AN OFFSET STRATEGY

While these technical and policy challenges are significant, they can be overcome. Interoperability is not an objective in itself—it is a means to an end, and that end is to achieve and sustain military advantage. Beginning in 2014, the DoD began an initiative known as the **Third Offset Strategy** that sought to create a military overmatch with both Russia and China. The name of the initiative conveys the fact that it was conceived as a continuation of previous strategic initiatives. While offset strategies have been used in the past, the current numbering only focuses on offset strategies used since the end of World War II. The **First Offset Strategy**, under this numbering system, occurred in the 1950s when President Eisenhower shifted U.S. strategy to rely more on nuclear weapons and massive retaliation to offset the Soviets' quantitative advantage in conventional forces. The **Second Offset Strategy** began in the mid-1970s under Secretary of Defense Harold Brown. Rather than relying mainly on nuclear weapons, the new strategy sought to offset Soviet numerical superiority in conventional forces by using a combination of stealth and precision-guided weapons to give U.S. forces a significant qualitative advantage—effectively making a smaller U.S. force more militarily effective than a larger Soviet one.

Interoperability is not an objective in itself—it is a means to an end, and that end is to achieve and sustain military advantage.

The Third Offset initiative, however, never fully coalesced into a strategy. While it succeeded in refocusing DoD on countering the challenges posed by Russia and China, it stopped short of articulating an overarching strategy. Instead, it identified a set of technologies that have the potential to provide an offset, and it focused the military on pursuing these technologies more aggressively. This ultimately manifested itself in the **2018 National Defense Strategy**, which called for increased efforts in "advanced computing, 'big data' analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future." It also recognized that, unlike previous offsets, the next offset strategy would likely rely on innovative technologies from the commercial sector.

WHY AN OFFSET IS NEEDED

An offset strategy leverages one's enduring strategic advantages and exploits the enduring strategic vulnerabilities of an adversary. For example, the First Offset leveraged the United States' advantage in nuclear weapons to counter the Soviet conventional forces. The Second Offset leveraged advances in stealth and precision to exploit the Soviets' enormous border and the vulnerability it represented for air defense. But the advantage provided by both of these offsets proved limited in duration because they fundamentally relied on new technologies. Technology conveys a fleeting advantage because it can be **stolen**, **reverse engineered**, or **countered** with other technologies—hence the need for a new offset strategy.

In the current strategic environment, China holds several strategic advantages over the United States that need to be offset. For example, its **economy** has grown faster and will soon exceed the United States in size, giving it the potential to devote more resources to defense. It already holds a quantitative advantage by fielding a larger military, **by some measures**. Moreover, China has developed a range of anti-access/area denial (A2/AD) weapons designed to exploit vulnerabilities in U.S. power projection capabilities, and its strategy is to **exploit temporal advantage** to achieve military objectives before U.S. and allied forces can effectively respond.

The United States also has strategic disadvantages that need to be offset. The United States is at a cost disadvantage due to decades of growth in **the cost per service member** and in the **operation and maintenance costs of forces**. This has gradually eroded the buying power of U.S. defense dollars, making it more expensive to support the same sized force over time, and it is the reason why military leaders **continually ask** for annual budget growth of 3 to 5 percent above inflation. Another disadvantage is that in a conflict with China, the United States will need to play an away game, operating forces over greater distances in a highly contested environment across all domains.

General Kenneth F. McKenzie Jr., Commander, United States Central Command (USCENTCOM), receives a brief given by U.S. and coalition forces participating in the field training exercise (FTX) during Bright Star 21 (BS21) at Mohamed Naguib Military Base (MNMB), Egypt, Sept. 11, 2021.

Photo credit: Spc. Amber Cobena

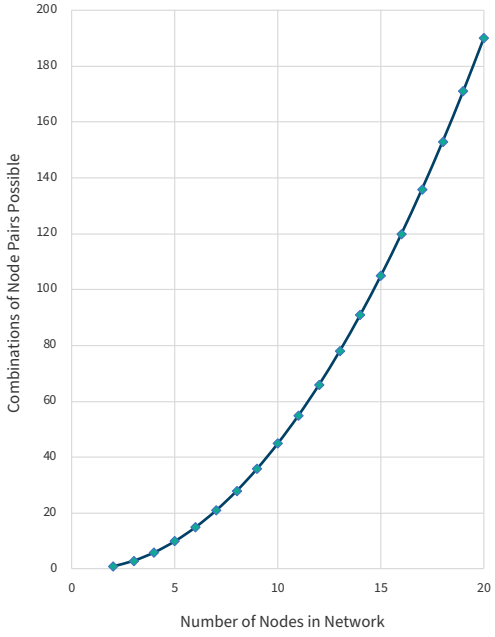
The United States, however, has many strategic advantages that

a new offset strategy can leverage, and China has many disadvantages that can be exploited. For example, the United States has a vast network of allies and partners that span the globe, providing access to geography and resources. Moreover, because these partnerships are founded on shared interests and values, they tend to be mutually reinforcing and stabilizing. China, in contrast, does not have comparable alliances, and its partnerships tend to be transactional and unequal.

TOWARD A NEW OFFSET

The Third Offset initiative highlighted the potential of leveraging artificial intelligence, big data analytics, and resilient communications for military advantage. Battle networks are what ties these technologies (and many others) together. What makes it an *enduring strategic offset* is integrating U.S. battle networks with those of allies and partners. Combined and interoperable battle networks leverage the United States' advantage with allies and partners in a way that cannot be easily replicated or countered. China can **attempt to build similar battle networks** of its own, but it cannot steal or reverse engineer alliances. And while China may become the largest economy in the world and use its resources to fund the largest military of any nation, it will still pale in comparison to the combined economic and military strength of the United States and its allies and partners.

Figure 3: Example Exponential Effect of Adding Nodes to a Network



Source: Authors' research.

China can attempt to build similar battle networks of its own, but it cannot steal or reverse engineer alliances.

As noted in a **previous paper in this series**, adding more nodes to a battle network increases both resilience and effectiveness. Designing battle networks for interoperability with allies and partners not only adds more nodes to the network, it also encourages new partnerships and deeper cooperation. Whereas the stealth and precision technologies at the heart of the Second Offset created a linear force multiplier effect, the ability to share data seamlessly across allied and partner battle networks creates a non-linear force exponent effect. It leverages the capabilities and capacity of each nation in the coalition, providing mutual benefits and ultimately enhancing deterrence.

CONCLUSION

The ultimate measure of success for both the First Offset and Second Offset Strategies is that they deterred direct conflict with the Soviet Union and, more specifically, Soviet aggression in Eastern Europe. The next offset strategy should similarly be focused on its ultimate objective—deterring Russian and Chinese aggression. As the **2018 National Defense Strategy** makes clear, the primary focus of U.S. strategy and defense planning is deterrence, and building interoperable coalitions is a key component of establishing a credible deterrent. As DoD continues to develop and experiment with different concepts and technologies for JADC2, it should keep this strategic focus in mind and make integration with allied and partner battle networks a top priority.

To demonstrate its commitment to allied and partner battle network integration, DoD should redouble its efforts to bring key allies and partners into early discussions, exercises, and experimentation for JADC2. For example, it could formally create positions for key allied and partner nations in JADC2 development programs, as the U.S. military did with the F-35 program management office. The inclusion of allies and partners early in the process demonstrates commitment and makes combined battle networks an integrated priority rather than an afterthought. Moreover, interoperability is easier to facilitate at the outset of network architecture design than it is to implement after the architecture has been established. But DoD should also be mindful to get its own

internal JADC2 organizational roles and responsibilities settled so that it can present a unified vision for JADC2 to allies and partners rather than a fragmented approach that differs from service to service.

Where interoperability challenges will be difficult, policy adaptations may prove harder. Policy hurdles are not problems to avoid in hopes that they will get better after DoD fully solves internal coordination issues among the services. They are issues that need to be tackled head on and in parallel with other efforts. As the recent experience in Afghanistan demonstrated, it took nearly a decade to establish a combined battle network with NATO and non-NATO coalition forces. The United States cannot wait until the initiation of a conflict to establish the necessary agreements and only then begin figuring out how allied and partner battle networks can be integrated. The speed of technological change and the pace of modern warfare mean that these agreements and architectures must be established well in advance.

DoD should focus its policy efforts on establishing more military and data-sharing agreements with nations beyond NATO and Five Eyes, particularly in the Indo-Pacific region. While the data show that the United States has historically emphasized military agreements with European countries, the shift in strategic focus to the Indo-Pacific region requires a commensurate shift in diplomatic efforts. What is needed are standing, long-term agreements to enable real-time intelligence sharing and battle network integration with more Indo-Pacific allies and partners. While ad hoc agreements for exercises or short-term contingencies are a step in the right direction, they are not a substitute for standing agreements that enable day-to-day deterrence operations. These policy agreements create the foundation upon which combined battle networks can be built and will ultimately enable an enduring strategic advantage for decades to come. ■

Todd Harrison *is the director of Defense Budget Analysis and director of the Aerospace Security Project at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Christopher Reid*** *is a military fellow with the International Security Program at CSIS.*

This brief is made possible with generous support from Lockheed Martin.

Cover Photo: Staff Sgt. Jessica Montaño/U.S. Air Force