JANUARY 2025

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Improving U.S. Intelligence Sharing with Allies and Partners

Author
Daniel Byman

A Report of the
CSIS Warfare, Irregular Threats, and Terrorism Program

January 2025

Improving U.S. Intelligence Sharing with Allies and Partners

Author
Daniel Byman

A Report of the CSIS Warfare, Irregular Threats, and Terrorism Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic and International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

This research was made possible by the support of the Smith Richardson Foundation.

The author would like to thank John McLaughlin and Norm Roule for their exceptionally helpful comments on previous versions of this paper, as well as CSIS Publications staff Hunter Hallman and Phillip Meylan, CSIS iLab staff Lauren Bailey, CSIS intern Skyeler Jackson for her assistance with graphics for this paper, and copyeditor Sarah Stodder. Thanks also to Patrycja Bazylczyk and Chris Park for their assistance with research on Poland and South Korea, respectively, and to Seth Jones and Sean Monaghan for their helpful reviews.

Many of the findings of this paper came from interviews with officials and experts in multiple countries around the world as well as in the United States. Given the subject matter, the interviews were conducted on the condition of anonymity, but the absence of specific names should not detract from the importance of their insights and my gratitude to them for their time and expertise.

Contents

Executive Summary

Intelligence sharing is vital to America's security.[1] Through it, the United States has gained information about security threats, identified opportunities to counter them, and provided similar benefits to allies—all at a relatively low cost. In addition, intelligence sharing has helped the United States and its allies form closer relationships overall, improving military, economic, and diplomatic ties.

Despite many joint collection and assessment successes, intelligence sharing sometimes fails to live up to its promise. As Sean Corbett and James Danoy—former senior British and U.S. intelligence officials, respectively—have written, "With few exceptions, and despite the best of intentions, intelligence sharing is uneven, remains the exception rather than the norm, and the prospect of simultaneity at the point of need is remote."[2] Because of its secretive nature, intelligence sharing generates fewer headlines and open complaints than other forms of cooperation; but in behind-the-scenes discussions with U.S. and allied officials and experts, frustration has been as common as praise. Although intelligence sharing has bolstered overall relations in many cases, systems of sharing frequently lack the bureaucratic foundations needed to enable smooth relationships.

The impact of sharing failures, though hard to measure, can be felt in several pernicious ways. Allies and partners may be slow to realize dangers posed by revisionist powers such as China, Russia, and Iran. Advanced planning based on varied intelligence assessments can hinder cooperation in a crisis. An ineffective division of labor may cause collection and analysis to suffer from both gaps and overlap. Intelligence sharing can bolster overall diplomacy between allies; without it, an important pillar of that relationship is weakened. But intelligence sharing problems may prove especially costly in an era of renewed great power competition.[3]

There have been many instances in which intelligence sharing has produced impressive successes. The "Five Eyes" (FVEY) partnership—a longstanding intelligence sharing arrangement between the United States, the United Kingdom, Australia, Britain, and New Zealand—has resulted in improved collection, better analysis, and greater burden sharing for its members. Outside of this longstanding partnership, the United States and its allies successfully expanded intelligence sharing after 9/11 and after the 2022 Russian invasion of Ukraine, suggesting that barriers can be overcome in moments of crisis.[4] Even so, significant intelligence sharing can be slow, as well as incomplete in its scope and scale.

Although allies and partners share the blame, the United States often makes it harder for well-meaning allies to cooperate with its intelligence services. This essay contends that U.S. intelligence sharing suffers in the following ways:

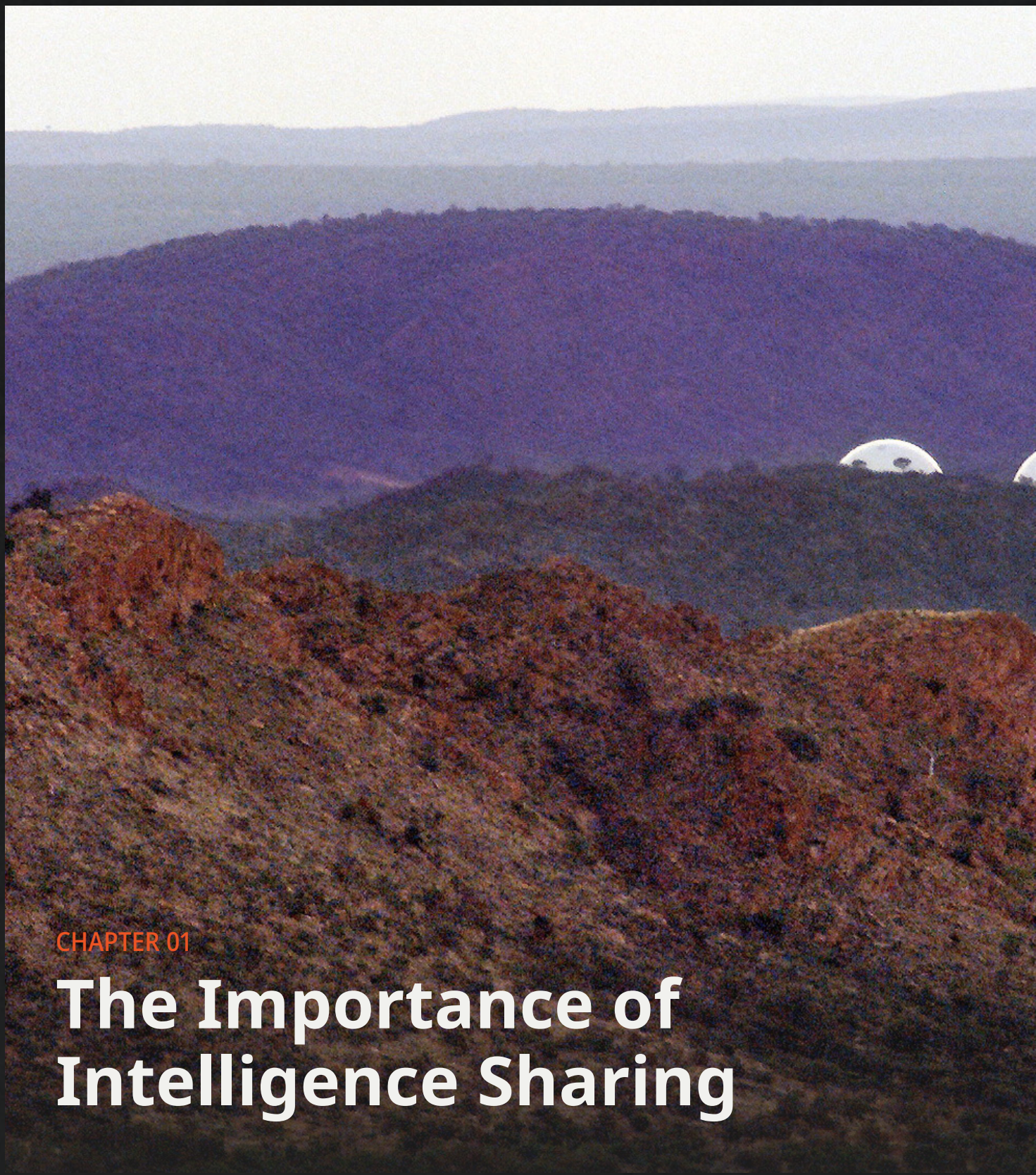
- **Trust problems**, often originating outside of intelligence circles and ranging from perceived interest differences to fears that the United States will use intelligence to manipulate decisionmaking
- **Diplomatic and political costs** to allies and partners should their relationship with U.S. intelligence become public
- **A U.S. release system that emphasizes security over sharing**, which often results in complex procedures and a default to Not Releasable to Foreign Nationals (NOFORN) even when the information does not involve highly sensitive sources and methods
- **Difficulties in interfacing with allied services** for resource, bureaucratic, and technical reasons
- **Unclear prioritization**, which results in insufficient incentives for mission-driven sharing
- **An under-resourced bureaucratic system** that at times undervalues intelligence sharing, allows different agencies to apply different standards, defaults to NOFORN, and imposes harsh penalties on individual officers for potential mistakes, creating strong incentives against sharing

To remedy these problems, the United States should take the following steps:

- **Improve prioritization of intelligence sharing with key allies** and encourage those allies to improve their technical systems and overall intelligence resourcing
- **Relax some security requirements with allies** and help them improve their own procedures, recognizing that intelligence sharing must be mission-driven and that security violations are likely as allies make these improvements
- **Alter U.S. procedures so that NOFORN is used less frequently** with non-Five Eyes allies, thus enhancing mission effectiveness
- **Share more information in low-risk areas**—such as climate security—in order to develop procedures and trust for higher-risk cooperation
- **Dedicate more resources and personnel** to increase the speed and scale of intelligence sharing within existing agencies
- **Expand high-level sharing beyond the Five Eyes partnership** on a finite set of issues (approved at the policy level), with particular emphasis on important partnerships in Asia (e.g., South Korea and Japan) and Europe (e.g., Germany and Poland)

In drawing these findings and making these recommendations, this report examines a range of academic, think tank, and government writings on intelligence. In addition, over 35 interviews were held with current and former U.S. and allied security experts, diplomats, and intelligence officials of varying ranks and seniority. Given the nature of the subject, the interviews were conducted off the record. No questions on collection, sources, methods, or other sensitive areas were asked or discussed.

This report consists of four sections. The first describes the importance of intelligence sharing for U.S. security. The second section describes current models of intelligence sharing, such as bilateral cooperation and the Five Eyes arrangement. The third section details a range of problems that plague current intelligence sharing efforts, using examples primarily from five countries: Australia, Japan, Poland, South Korea, and the United Kingdom. Drawing on this analysis, the essay's fourth section offers recommendations for improving intelligence sharing and notes factors that are unlikely to change.



CHAPTER 01

The Importance of Intelligence Sharing

The radar domes of the U.S.-Australia joint miltary base at Pine Gap, photographed near Alice Springs, central Australia, January 14, 1999.
TORSTEN BLACKWOOD/AFP VIA GETTY IMAGES

Sharing intelligence with the right partners offers many potential benefits. No intelligence service knows everything, and even small nations have valuable human sources or other assets in their own neighborhoods.[1] As a former head of the UK Secret Intelligence Service (SIS) put it, intelligence is "a team sport."[2] As scholar Jennifer Sims points out, intelligence liaison can lower overall collection costs, improve timeliness, and facilitate effective joint operations. Intelligence partners may also have advantages in language skills (a particular U.S. weakness), historical relationships, and access.[3] Estonia, for example, has a superb service with many Russian speakers and a longtime Russian focus.[4] Some allies have an official presence in places like Iran and North Korea, where direct U.S. access is limited to nonexistent. Allied access is also vital in places like China, where any American—especially an American official—is constantly monitored.[5] Some intelligence services, such as those of the United Kingdom, have global reach.[6] In addition, access and capabilities can take years to build, so it is often vital to draw on partners with preexisting assets in a crisis.[7]

The counterterrorism era yielded numerous instances of successful intelligence sharing that made the United States and its partners safer. Allies generated intelligence and often served as the tip of the spear, arresting or otherwise disrupting suspected terrorists. The capture of terrorists such as David Headley and Najibullah Zazi relied heavily on British intelligence, and Saudi

Arabia played an important role in preventing terrorist attacks from Al Qaeda in the Arabian Peninsula.[8]

Intelligence sharing is also vital for effective coalition military operations. U.S. military campaigns against the Islamic State and Al Qaeda have demonstrated the value of such sharing for counterterrorism purposes. The U.S.-Poland ballistic missile defense agreement, for example, requires intelligence cooperation to ensure the security of U.S. installations, launchers, and technical data.[9] Similarly, the United States and South Korea share intelligence on space as part of a broader effort that includes training and exercises.[10] Beyond tactical sharing of battlefield information, intelligence exchanges also facilitate joint planning.[11] As one European official put it, "All plans depend on intelligence. Bad intelligence means bad plans."[12] U.S. deployments related to Russia and China often depend on effective intelligence relationships with regional states.

Such relationships can also bolster overall diplomacy and alliance strength. One former allied official noted that U.S. assessments shaped their own country's worldview in dozens of small ways that, over time, brought the two into greater alignment.[13] Intelligence relationships facilitate trust that can be useful for negotiations on more traditional foreign policy issues such as peace talks between belligerents.[14] Polish officials noted in interviews that intelligence cooperation was an important part of their country's overall relationship with the United States.[15] Over time, shared intelligence also contributes to a shared worldview and set of threat perceptions. As former Secretary of Defense Donald Rumsfeld once noted, "To the extent we are all working off the same set of facts, or roughly the same set of facts, the people from our respective countries tend to come to roughly the same conclusions, and to the extent we're not working off the same set of facts, we tend not to."[16]

Great Power Competition and Intelligence Sharing

The 9/11 attacks led to a massive change in intelligence liaison, with terrorism-related intelligence coming to the fore.[17] Attention focused on improving liaison with countries that had a jihadist presence or were otherwise on the front line of the struggle against terrorism.[18] In contrast to the Soviet Union in the Cold War–era, Al Qaeda, the Islamic State, and other jihadist movements had little in the way of sophisticated counterintelligence: Information might be revealed to an adversary through leaks, but the odds of an Al Qaeda penetration of U.S. or other allied services were low. Jihadist signals intelligence (SIGINT) collection was also limited, especially when compared to great power adversaries' capabilities.

Great power competition, however, poses a new set of intelligence challenges.[19] Multiple U.S. administrations have tried, not always successfully, to reduce focus on the greater Middle East. As in the Cold War, Russia has been an area of increased emphasis, with allies in Europe posed to play a critical role in confronting Moscow. Strong bilateral relationships, robust alliance structures like NATO, and other arrangements that involve intelligence—many of which were developed during the Cold War—will serve the United States well.[20]

China, however, is a far bigger long-term concern, and one that Cold War structures will not meet. Many European allies and partners have shared intelligence with the United States and each other for decades. East Asian allies and partners, in contrast, have limited collection capabilities; they have not had robust sharing relationships with the United States for long periods of time and share even less intelligence among themselves. Asian allies also have complicated relationships with China, given its economic importance and its increasingly dominant position regionally.[21]

Security risks are also much greater than they were in the post-9/11 era. China and Russia both have effective intelligence and counterintelligence services. They guard their information more effectively than the post-9/11 jihadist movements did, which creates a need for more sophisticated collection efforts. In addition, they are aggressively trying to penetrate U.S. services, as well as those of U.S. allies and partners.[22] As a result, the risk of U.S. information ending up in adversaries' hands is much greater now than in the era when counterterrorism was the priority.

A Turning Point for Intelligence Cooperation?

Just as the start of the Cold War and the events of 9/11 led to significant intelligence liaison changes, recent international turmoil and changing U.S. priorities offer opportunities for the restructuring and improvement of intelligence sharing. The Ukraine war has highlighted the Russian threat, energizing European states and increasing their day-to-day security cooperation with both the United States and one another. In Asia, the rise of China has alarmed states as diverse as Australia, Japan, the Philippines, South Korea, and Taiwan, creating the potential for greater cooperation against a shared threat. The signing of the Australia-United Kingdom-United States (AUKUS) agreement in 2021 is one sign of how regional relationships are being reordered and institutionalized.[23] However, as one official involved in AUKUS noted, even as arms sales and defense cooperation have improved dramatically, "intelligence has not kept pace."[24]

The Scale of Intelligence Sharing and U.S. Commitment

Although this paper focuses primarily on ways to bolster intelligence sharing, it is important to acknowledge the considerable and usually fruitful sharing that already exists with partners. The United States regularly engages with numerous civilian and military partners abroad, sharing finished human, signals, geospatial, and other intelligence on a daily basis. This sharing often increases in response to crises, such as Russia's invasion of Ukraine, or to growing threats, such as Iran's malign adventurism.

The intelligence community is aware of the depth of the challenge. Within the U.S. system, the Office of the Director of National Intelligence (ODNI) and National Counterterrorism Center (NCTC) were created to overcome internal stovepiping, while combatant commands have created fusion cells with partners to ensure information flows during war.

Intelligence community members often have a strong understanding of partner needs. Country teams focus on how to manage liaison relationships, a process augmented by liaison visits and analytic exchanges. Senior officials regularly discuss what to share and what not to share, making decisions based on their own impressive backgrounds in the countries and issues in question.

Because this paper focuses on ways to improve sharing, interview questions often zeroed in on problems. However, the vast majority of the interviewees stressed the value of U.S. intelligence sharing and noted that many officials were highly committed to a strong relationship between the United States and its allies.

CHAPTER 02

Intelligence Sharing Structures

Aerial view of the Government Communications Headquarters in the United Kingdom, on October 6, 2023.
DAVID GODDARD/GETTY IMAGES

Intelligence scholar H. Bradford Westerfield notes that the particulars of intelligence liaison vary considerably and can include sharing information, working together on operations, and full-fledged joint collection. Liaison may also involve training, financial support, and providing technical or other supplies.[1] Sometimes arrangements are institutionalized via a memorandum of understanding or similar means; sometimes they are informal.[2] At times agencies exchange finished assessments; but one former intelligence official interviewed stressed the value of sharing raw intelligence, which enables agencies to "check each other's homework" and even source knowledge.[3] In other cases, sharing may involve requests for political support, military equipment, or other non-intelligence benefits.[4]

Bilateral Structures

Bilateral cooperation is usually the preferred form of intelligence liaison. This is primarily for security reasons, though it also proves convenient at times for two countries to unite on a particular issue of mutual concern. The more widely information is disseminated, the more likely it is to be revealed through spying, media leaks, or other unauthorized disclosures.[5] Historically, many U.S. intelligence engagements in Asia have been bilateral. The United States has long had strong relations with Japan and South Korea, but information has largely been shared directly, rather

than as part of a larger grouping. For example, the United States gives South Korea the critical signals intelligence it lacks, while South Korea provides human intelligence in exchange.[6]

Multilateral Structures

The United States has multilateral exchanges via alliances such as NATO. Similarly, Europe has arrangements like the Berne Group for sharing intelligence.

Some U.S. multilateral sharing relations are stunted due to limited trust in allied security systems and procedures, fears of adversary penetration, or concerns that allies' different interests might lead them to disclose information to adversaries. Often these arrangements facilitate the exchange of overly broad reports that do not offer detailed intelligence, for fear of information being compromised.[7]

In general, because of information security concerns, larger circles tend to lead to weaker cooperation. As Sims contends, "The quality of the exchange will generally be determined by the least trusted (most suspect) member of the group."[8] As a result, multilateral liaison often leads nowhere, with members fearing that the weak security of one participant will compromise the entire group. This is particularly true of more sensitive collection and sourcing discussions.

The Five Eyes

There are, however, impressive exceptions to the general dominance of the bilateral sharing model. The Five Eyes alliance, which grew out of the U.S.-UK World War II partnership and has been around for over 70 years, is often held up as the gold standard for intelligence sharing. As scholars have noted, the Five Eyes "is unique in the combination of its longevity, its resilience to changing global circumstances, and its ability to survive periodic tensions as well as maintain an ongoing similarity in the worldviews of its membership."[9] The countries involved share intelligence related to foreign communications and methods of collection. They also share finished intelligence products.[10] A senior British intelligence official pointed out that the U.S.-UK SIGINT relationship is so strong that "customers in both capitals seldom know which country generated either the access or the product itself."[11] Although the historical emphasis on signals intelligence remains important today, Five Eyes members also share assessments, as well as procedures and terms for classifying information.[12]

The Five Eyes alliance has achieved these successes for several reasons:

- The Five Eyes countries share values, interests, and language; longstanding institutionalization has further strengthened bonds. The United Kingdom helped establish U.S. and other allied intelligence organizations during and after World War II, often using British models, and this shared foundation has made later cooperation easier.[13]
- The division of labor is meaningful among Five Eyes members, with different countries having responsibility for different parts of the world. For example, according to intelligence historian Corey Pfluke, Australia monitors South and East Asian communication, while New Zealand covers the South Pacific and Southeast Asia. An Australian Department of Defense study found that "the US looks to Australia for all SIGINT in our region of principal coverage and does not duplicate the effort," citing Islamic extremism as an example.[14] Partners respond to each other's needs when they do not have their own reporting.[15]
- The Five Eyes share exchange liaison officers, do joint operations, have joint communication channels, and jointly staff many important facilities.[16]
- The Five Eyes can "follow the sun," passing off a task from one partner to another for around-the-clock operations.[17]
- Over time, the Five Eyes' shared activities, personnel swaps, and institutionalization have generated personal relationships, which in turn have led to greater trust among institutions, understanding of different systems, and opportunities for bureaucratic work arounds.[18]
- Five Eyes nations have reportedly agreed not to spy on one another.[19] This "no-spy" pact further

bolsters confidence that intelligence officers from Five Eyes countries are there to help with common problems, not to secretly collect intelligence of their own.

- Five Eyes nations respect each other's areas of influence. For instance, one U.S. official noted that a decision in Indonesia would never be made without input from Australia.[20]

It is important to note, however, that the Five Eyes relationship has endured many problems over the years. During World War II, the United Kingdom had security concerns about passing analysis to the United States.[21] Simultaneously, both the United States and the United Kingdom had concerns about sharing SIGINT with Australia due to lax security procedures there. As a result, they restricted access, excluding much of Australia's cabinet.[22] Political differences also shaped the early relationship. London did not circulate Joint Intelligence Committee papers on Palestine during partition because of perceived "Jewish sympathies" in Washington.[23] Over the years, all five countries have had serious security lapses that have compromised sources. Such lapses have included the "Cambridge Five" in the United Kingdom, Aldrich Ames and Ana Montes in the United States, the Soviet mole Ian George Peacock in Australia, a 2021 Chinese cyberattack that infiltrated New Zealand government systems, and the connections of numerous Canadian politicians to Chinese intelligence officers.

The relative importance of some Five Eyes members may shift with the rise of China. One expert noted that concerns about China have already "turbocharged" the Five Eyes, with Australia in particular playing an unprecedented role.[24] New Zealand, a less important player in the Cold War and post–Cold War eras, given its distance from the Soviet Union, is now situated to be an important intelligence partner in the South Pacific, Antarctica, and various parts of Asia, although resources remain an issue for Wellington.[25] Conversely, Canada's importance may decrease relative to that of other members given its distance from Asia. As existing relations change, more complaints are likely. With new priorities and additional points of contact emerging, new points of friction will arise.[26]

Other Sharing Arrangements

In addition to the Five Eyes, press reporting indicates that the United States has other circles of information sharing. The so-called "Nine Eyes" partnership includes Denmark, France, the Netherlands, and Norway, in addition to the Five Eyes countries. The "Fourteen Eyes" adds Belgium, Germany, Italy, Spain, and Sweden.[27] These relationships, however, are not as institutionalized as the Five Eyes. The United States also recently organized the Framework Intelligence Group to facilitate the release of Secret-level information to 14 member states: the Five Eyes, Belgium, Denmark, France, Germany, Italy, Japan, the Netherlands, Norway, and Spain. Many instances of multilateral sharing are ad hoc and occur during crises. U.S. Central Command (CENTCOM) shared information related to Iranian ballistic missiles in order to help Israel defeat Iran's attacks in April and October 2024. The United States, the United Kingdom, France, and Jordan all provided capabilities to assist Israeli air defense, which in turn required intelligence sharing among these countries.[28]

The United States has also tried to foster intelligence relationships among and between its partners. Historically, Japan and South Korea have each had bilateral intelligence relationships with the United States, with any information relevant to the other shared only via transmission through Washington. In 2016, the two Asian countries agreed to the General Security of Military Information Agreement (GSOMIA), allowing them to share intelligence on North Korean military and nuclear activities with each other.[29]

Allies often have important relationships of their own. Taiwan and Japan have long had a strong bilateral intelligence relationship.[30] Similarly, although the United Kingdom's military capacity has declined, it maintains a strong intelligence capacity, which it uses in bilateral relationships to advance its interests.[31] Five Eyes partners also have their own liaison partners: Canada and Australia, for example, each have relationships with over 100 countries.[32]

CHAPTER 03

Common Intelligence Cooperation Problems

A South Korean protestor holds a placard showing a caricature of US President Donald Trump during an anti-US rally in Seoul on August 14, 2017.
JUNG YEON-JE/AFP VIA GETTY IMAGES

The United States and its allies and partners suffer from numerous problems in intelligence relationships. Some of these are structural, involving different interests and cultures, and are difficult or impossible to overcome. Still other problems—notably those regarding security procedures—involve tradeoffs, with greater sharing leading to higher chances of valuable human sources and sophisticated and expensive technical methods being lost. In other cases, however, the problems are own goals, with procedural or bureaucratic issues causing numerous complications. These issues, detailed below, can be grouped into five categories: trust concerns, autonomy concerns, security barriers, incompatible interfaces, and bureaucratic barriers.

This section expands upon those problems and tensions, using the experiences of Australia, Japan, Poland, South Korea, and the United Kingdom. These countries were chosen for several reasons. Two of them—Australia and the United Kingdom—are long-standing Five Eyes partners. The issues they experience suggest how problems can endure even within the closest intelligence relationships. Japan and South Korea also have a close relationship, but one in which intelligence sharing is less institutionalized, even as the threat of China grows.[1] Finally, Poland is a relatively new ally, but its intelligence importance has increased considerably as the United States has renewed its attention on the Russian security threat.[2] Many of these countries have significant problems of

their own that raise legitimate complications for intelligence sharing, but this paper focuses primarily on issues that affect how the United States might improve sharing on its end.

Obstacle 1: Trust Concerns

While even close allies often have trouble fully trusting one another, the issue of trust is more significant between countries with histories of animosity. Common problems in this area include general mistrust due to different histories and perceived interests; concerns about U.S. arrogance and potential to use intelligence to manipulate; and concerns that the United States will spy on the partner country.

General Mistrust

Allies have their own interests, and even when these interests align with the United States', they are rarely identical. One former allied official put it succinctly: "Alliance is not allegiance."[3] Henry Kissinger also once touched upon this point, remarking that "there is no such thing as friendly intelligence agencies. There are only the intelligence agencies of friendly powers."[4]

As one Asian government official noted wryly, "Few countries are so unmolested by thoughts of history as the United States."[5] U.S. dignitaries, the official noted, often say, "That was so long ago," or "But now we have shared interests." Yet this rhetoric is not enough to underpin alliances. Radek Sikorski, Poland's former secretary of defense, wrote in 2007 that "just as the Holocaust is the formative experience even for Jews who are too young to remember it, so Poland is haunted by the memory of fighting Hitler alone in 1939 while our allies stood by."[6] Such historical imprints can sometimes be unwittingly overlooked by the United States: one Polish official, for example, recalled that the United States canceled its missile defense plans with Poland on September 17, 2009, the 70th anniversary of Russia's invasion of Poland.[7]

Part of the disconnect is simply due to the global nature of U.S. interests, as contrasted with the regional views of most other allies. One South Korean official noted that "the United States will be distracted" from its current focus on China because of its interests in Europe and the Middle East.[8] Conversely, Polish officials worry that U.S. focus on China will leave Poland vulnerable to Russian aggression, while British officials are concerned that a China emphasis will diminish their value relative to U.S. allies in Asia.[9] Middle Eastern governments, for their part, worry that Russia and China will lead to U.S. neglect of their region. A former South Korean official, meanwhile, noted that U.S. efforts to de-escalate in Ukraine and the Middle East raised concerns that the United States would not give South Korea full support in a crisis.[10]

Different interests, of course, are not new. The Five Eyes, rightly touted as a landmark intelligence sharing success, involves countries with varied interests. The United States and the United Kingdom, for example, have had different views on trade, human rights, and conflicts like Vietnam, yet the intelligence relationship endured.

Mistrust is often most pronounced when partners consider other U.S. allies. In general, many countries do not see eye to eye with their neighbors and thus are more willing to share with the United States than with one another.[11] A South Korean official noted that his country is afraid of "*all* of the countries in the region."[12] In general, Asian countries all have different views of Japan, for example—views shaped by geography, interests, and history.[13] In the case of South Korea, the country has long harbored hostility toward Japan due to its World War II brutalities and prewar colonialism; this has made security cooperation with Japan a politically sensitive issue, made worse by a sense in South Korea that Japan has not fully renounced its past imperialism.[14] One South Korean expert noted that this concern was "nonsense," but that its impact was nevertheless real.[15] As a result, the staying power of the U.S.-backed GSOMIA is uncertain. One analyst called these ups and downs a "'one step forward, two steps back' situation."[16]

Concerns About Arrogance and Manipulation

One former U.S. official noted that the United States often believes it understands the interests of allies better than they themselves do—even as U.S. policies and priorities regularly flip flop. U.S. stances are,

or can be perceived as, arrogant and uninformed at times: a "Daddy knows best" approach, as the official described it.[17]

Yet it behooves the United States to listen to allies. U.S. and former Australian officials noted that Australia was often ahead of the United States in recognizing the growing China threat.[18] A Polish official recalled that under President Trump, the United States regularly emphasized the hybrid threat from Russia even as Poland urged more focus on the conventional military threat.[19] A South Korean official pointed out that North Korea, not China, is usually Seoul's top concern, despite U.S. efforts to shift the country's perceptions.[20]

Some allies worry that the United States selectively shares only the intelligence that supports preferred U.S. policies. South Korean analysts, for instance, fear that the United States has misrepresented its intelligence to slant Seoul's policy decisions on North Korea. South Korea has limited satellite imagery and SIGINT, and thus finds it hard to challenge U.S. intelligence findings that draw on these sources.[21] Some in South Korea claim that the United States knowingly shared false information that North Korea sold nuclear materials to Libya (when the true culprit was Pakistan) because Washington wanted to shore up Seoul's fears of its northern neighbor. Conversely, South Korean reporting claims that in 1996, when North Korea sent commandos into South Korea using a submarine, Washington did not provide Seoul with detailed intelligence to avoid escalating tensions.[22] This concern contributed to South Korea's decision to develop its own SIGINT capability.

Fear of Spying

U.S. spying on allies raises another security complication. In 2013, leaks indicated that the United States was monitoring the phone of German Chancellor Angela Merkel. In 2023, the *Korea Herald*, drawing on Discord leaks, revealed information that indicated that Washington was spying on South Korea—a concern that exacerbated South Korean fears.[23]

Liaison itself can facilitate spying. Liaison services can use their access to another country's intelligence personnel to try to recruit them as spies.[24] This complication can go both ways: a South Korean official, for instance, noted that Seoul also tries to spy on and influence the United States.[25] However, the U.S. "no spy" pledge with the Five Eyes helps offset this concern.

Sharing also creates a risk of losing spies. One non-U.S. officer noted that smaller nations feared that revealing their sources to the United States might open the door for Washington to recruit them, outbidding their original affiliates.[26]

Obstacle 2: Autonomy Concerns

The U.S. intelligence community commands vast resources in comparison to its partners.[27] A senior UK intelligence official noted that U.S. intelligence has a bigger budget "than the UK Ministry of Defence, armed forces, aid budget, Foreign Office and intelligence agencies combined."[28] A 2017 report on the Five Eyes indicated that the United States provided 90 percent of the intelligence shared with Australia in that alliance.[29] One study from 2016 found that 85 percent of South Korea's SIGINT and IMINT on North Korea came from the United States.[30] Similarly, Japan has significant weaknesses in its SIGINT and cyber capabilities, which are offset by U.S. support.[31]

In general, the United States collects, analyzes, and disseminates far more intelligence than its allies, which makes it a highly desirable partner. A downside of this, however, is that allies fear becoming too dependent on U.S. intelligence. In response to concerns about intelligence autonomy vis-à-vis North Korea and China, South Korea has tried to develop its own intelligence, surveillance, and reconnaissance (ISR) capabilities, overlapping those of the United States.[32] Some Australian analysts fear that they are losing autonomy in intelligence and policy, citing their government's decision to go to war in Iraq based on incorrect U.S. intelligence.[33]

This fear has precedent. During World War II, for example, Australia focused on Japanese traffic analysis; when the United States temporarily pulled back from the Pacific after the war, Australia was left with little capacity for the SIGINT tasks, such as cryptanalysis, that the United States had handled.[34]

Obstacle 3: Security Barriers

When sharing intelligence, U.S. officials rightly worry that partner nations may have security lapses that lead to adversary penetration, leaks to the media, or both. In the end, security and intelligence sharing involves a risk-reward trade-off. Even if allies exercise careful information security, counterintelligence concerns remain a harsh reality. By sharing more, the United States increases the risks both to the lives of sources and to the value of a multibillion-dollar technical system. As such, a security mindset often dominates intelligence sharing. The more sensitive the intelligence platform or method, the greater the concern.

Many partner countries have weak counterintelligence, leaving them vulnerable to adversary intelligence services. Because many important countries are frontline states, they are often especially vulnerable to adversary penetration. Post–Cold War Poland, for example, has had numerous Russian penetrations of its intelligence services and security establishment.[35] Some allies vital to the struggle against China also have weak security. One foreign official noted that their service would be reluctant to share with the Philippines, given Chinese penetration there.[36] Questions about sharing sensitive information with Taiwan at times produced laughter from interviewees. Within NATO, both Turkey and Hungary have cooperated with Russia diplomatically and, at times, on security, making other countries reluctant to share information for fear of it being passed to Russia.

The United States, too, has counterintelligence problems that pose dilemmas for allies: U.S. leaks are a periodic problem, both in the intelligence community and at political levels.[37] When information regarding secret U.S. detention sites in Poland leaked in 2005, Poland denied this (helpfully, from a U.S. point of view). Yet later revelations of Polish involvement led to concerns in Poland about the security of Polish troops operating in support of U.S.-led missions in the Middle East.[38] The 2010 WikiLeaks publication of massive amounts of U.S. intelligence related to Iraq and Afghanistan and Edward Snowden's 2013 leak of volumes of highly classified data are among the many examples of information from allies becoming public. In the Snowden case, some of the information allegedly came from Five Eyes sources, and the leaks hurt allies' intelligence output.[39] Similarly, the 2017 leaks to U.S. media of sensitive British intelligence and President Trump's leak of Israeli information related to Syria both angered partners and raised questions about U.S. reliability.[40] Reports that the National Security Agency (NSA) had shared the personal information of Canadians citizens led Canada to put data sharing on hold with Five Eyes partners.[41] In almost all of these cases, however, the impact of the leaks were short (term and cooperation resumed in the long term.[42]

Leaks also feed conspiracy theories, which are only exacerbated by "no comment" responses.[43] Even worse, as one foreign official noted, "Security leaks from U.S. sources lead to a clamp down on what can be shared with foreign partners." These situations can lead to a general tightening of all information sharing, even to partners who are not responsible for the problem.[44]

The United States also has far more legislative oversight of its intelligence agencies than other allies do. This often raises fears among partners that Congress will reveal information they provide or otherwise compromise security—a fear that is magnified by the executive branch's frequent blaming of Congress for leaks, many of which actually stem from the executive branch itself.[45] In addition, Congress often wants to have it both ways, pushing cooperation while also blaming the intelligence community when such cooperation leads to security lapses.

In rarer cases, foreign intelligence may also be revealed in court cases if it is considered by the court to be legitimately relevant to a trial.[46] Often this is related to counterterrorism or counterintelligence allegations against a citizen of another country, when the defendant's right to a fair trial trumps security concerns.

Obstacle 4: Incompatible Interfaces

Even when both sides are committed to sharing information, doing so can be difficult in practice. Common problems include a lack of secure technical systems, incongruence in counterpart organizations, differing political and legal mandates among organi-

zations, and diverging modes of collection, analysis, and information storage.

Lack of Secure Technical Systems

For intelligence to be shared, computer and other information systems must be able to connect in a sufficiently secure manner. Some allies, such as the United Kingdom and Australia, have special access to the Secret Internet Protocol Router Network (SIPRNet), a secure network for conveying classified material.[47] There is now also a SIPRNet option to quickly label information as releasable to Japan as part of a drop-down menu, an important step that puts it more on par with the Five Eyes.[48] Taiwan has reportedly upgraded its computer system to exchange real-time intelligence with Five Eyes.[49] NATO allies, on the other hand, use the Battlefield Information Collection and Exploitation System (BICES).[50]

Despite such measures, the incompatibility of different technology systems is a major obstacle to intelligence cooperation, hindering both the speed and scale of information sharing. As one Five Eyes official noted, "Just because we have an intelligence sharing agreement doesn't mean we have intelligence sharing systems."[51] Usually the problem is a "multitude of mini-problems," another official noted. [52] Some information systems have drop-down menus that easily allow sharing with various allies, while others do not.[53] One U.S. official noted that the systems are hard to use for sharing, and it is often difficult to know how to get information. The same official also noted that while the system works half of the time, requests are automatically rejected the other half of the time for unexplained classification reasons.[54] Indeed, one Five Eyes official noted that information sharing is often better at the Top Secret level than at the Secret level because of the historical sharing of SIGINT.[55] Information often cannot go from one country's system to another's, even when both sides want to share. In some cases, certain forms of sharing do function well, such as email, but other forms, such as shared drives, aren't present.[56] Problems still occur, even with close allies on time-sensitive issues, because systems do not align.[57] Japan, for instance, has few intelligence sharing terminals in contrast to other allies, because many such terminals are allocated via NATO.[58]

In general, complexity grows when information is shared with more than one national actor. Countries may have sharing agreements with the United States, but often do not have them with each other. As such, they must frequently send information to the United States for transmission to a third country, rather than work directly with that country. [59]

The cost of this communication problem is likely to increase as the role of technology in information processing grows. Manual disclosure to foreign partners, for example, works poorly when there are vast amounts of information, much of which is now processed by artificial intelligence (AI).[60] As many U.S. allies under-invest in technology systems, these gaps are likely to grow.[61]

Lack of Bureaucratic Congruence

There is variation in bureaucratic congruence among U.S. partnerships, often depending on levels of historical cooperation. Cooperation between the NSA and its British counterpart, the Government Communications Headquarters (GCHQ), is excellent; Defense Intelligence Agency (DIA) and National Geospatial-Intelligence Agency (NGA) cooperation with their UK counterparts is strong; CIA cooperation with MI-6 is solid; FBI cooperation with the Security Service is relatively weak, however, as the two agencies have had fewer reasons to connect over the years. Not surprisingly, the technically oriented collection agencies have the most sophisticated and seamless systems for information sharing.[62]

Many allies have balkanized intelligence services. Although some, like Australia, have the equivalent of a DNI, there is no South Korean administrator who acts as a central coordinating authority between intelligence agencies. As such, the DNI in Washington has no counterpart in Seoul with whom he or she can meet to discuss and negotiate the intelligence relationship. Successive U.S. DNIs have only publicly met with the South Korean president during their visits to the country, but a country's president is not focused on intelligence coordination.

Organizational incongruency extends to individual intelligence agencies. The director of the NSA is a four-star general; meanwhile, a two-star general heads the Defense Security Agency (DSA), the South

Korean SIGINT body. There has been no public interaction between the respective heads of the NSA and DSA. Instead, the special United States liaison advisor Korea, an NSA contingent in the country, has facilitated SIGINT cooperation since the end of the Korean War.[63] While the technical capacity to share large volumes of collected intelligence exists, organizational differences create issues.

A lack of internal integration can also create difficulties for external sharing. Countries often do not share information well internally, which makes it harder for them to share information with the United States. (The reverse is also true, and this problem applies just as much to the United States in its attempts to share information with other nations). At least several U.S. partners have had to better integrate their own intelligence and threat assessments in order to share more effectively with partners.[64] When a fusion center or similar location exists to centralize information, sharing becomes easier because there are fewer actors with whom to coordinate, as well as a common set of security procedures.[65]

Japan, for example, is highly siloed, with five major intelligence agencies. These often do not share with one another, and thus it is not surprising that they often do not share with the United States—or that when they do, each has its own independent relationship.[66] Poland, too, lacks a clearinghouse for much of its information. As a result, collection from separate services is often duplicative, and the information collected is often not shared internally or with the United States.[67]

Because of this technical and procedural complexity, personal relationships matter tremendously, as they help ensure coordination through bureaucratic work-arounds. As one former senior U.S. official declared, "So much is personality based."[68] In U.S.-Australia collaboration, Pine Gap is a key location for joint collection; it also serves as a space for American and Australian intelligence personnel to form trusting professional relationships. Foreign military and intelligence officials play vital roles in explaining their countries' perspectives to U.S. personnel. On the other side, the host country's knowledge of local U.S. chiefs of station is often vital, as is the knowledge of other leading defense and intelligence officials.[69]

In many cases, however, U.S. officials deployed to foreign countries do not speak the language, which limits the creation of personal relationships, and overall communication. Language facility also demonstrates respect for host cultures. Local familiarity can often vary by service: One interviewee noted that U.S. Navy officers and Marines know Japan's history and interests well, for example, while the knowledge of Army officers is more limited because the historical relationship is not as strong.[70]

Different Political Mandates Among Organizations

Part of why the Five Eyes works well is that intelligence agencies play similar roles in member governments, in which intelligence is both regularly used and largely depoliticized.[71] In other partner countries, including many democracies, intelligence services are more politicized and thus more likely to change course with political winds. This has led to concerns in the United States about sharing information with these partners, and especially about bolstering their capabilities.

In South Korea, the transition to democracy has led to more oversight and restrictions on domestic spying. Despite these restrictions, South Korean intelligence has been involved in illegal wiretapping and disinformation operations in presidential and other elections.[72] One 2018 study found that almost all presidents of South Korea have not permitted the country's intelligence apparatus "to adhere strictly to its legal mandate of non-intervention in domestic politics."[73]

Some important countries concerned about Russian and Chinese aggression are themselves autocracies, while others have political systems that, while democratic, are more prone to abuse of power and human rights violations, often with intelligence services implicated. In Poland, when the Law and Justice Party (PiS) arose in the early 2000s, it made claims that the secret services had penetrated the country's economic and political systems and were often in league with Russia. When the PiS won elections, it argued that cleaning house required a purge of the intelligence agencies, with one leading PiS critic of the services claiming that the services' main purpose was as "a le-

ver for pursuit of party politics and informal power networks that managed to capture the Polish state."[74]

Different Modes of Collecting, Analyzing, and Storing Information

Different intelligence services have different historical traditions, and these can make coordination with other services difficult. Sir Stephen Lander, the former director general of the UK Security Service, remarked in 2004 that some countries "collect haystacks and store them, while others collect hay and store needles, while others again only ever collect needles and not very many of them. The risk of sharing haystacks with needle keepers is that they would not be able to use the material effectively or would be swamped."[75] Another challenge is between states that divide domestic and foreign intelligence, such as Canada, and those that do not, which creates collection and dissemination restraints for both partners.[76]

Obstacle 5: Bureaucratic Barriers

U.S. information-sharing procedures also create additional—and at times unintended—barriers to intelligence cooperation. Problems include strong incentives to classify information as NOFORN, overall system complexities, and the proliferation of veto players in the U.S. system.

NOFORN Incentives

The United States has created a labyrinthine set of rules that govern the sharing of information, imposing severe limits within broader policy guidance from senior U.S. officials (who, as one official noted, often create or endorse many of these rules). The United States, as one U.S. official put it, "does not have any info sharing policies at all. It has information security policies and information sharing exceptions to these policies."[77] As Corbett and Danoy argue, "The policy as it stands can be interpreted to support a default setting to NOFORN."[78] As a result, important information regularly is not shared or, almost as bad, takes far too long to be shared, which greatly reduces its value.

In general, as a former senior U.S. official put it, there is "wild overclassification" in the United States, and the tremendous complexity of rules governing information sharing adds to this problem. The official went on to note that the United States "no longer knows what its intelligence crown jewels are."[79] This has become more and more true as the amount of classified information has ballooned, with far more personnel seeking access to it at their jobs, thus increasing the risk of compromise.[80] As journalist Patrick Radden Keefe contends, "For any government officer making a quick decision in the course of a busy workday, the penalties for underclassifying are quite salient, whereas penalties for overclassifying do not exist."[81]

Often, bureaucratic incentives for working-level officials are the problem. "A Four Star can say 'release everything,' but some guy in tennis shoes [in a different bureaucracy] sees a missing label and kills it," said one foreign intelligence officer.[82] Another foreign intelligence officer noted that senior U.S. officials regularly send out directives calling for more sharing with allies, but in practice little changes: "The bureaucratic reluctance is in stark contrast to the strategic guidance. The people who manage risk emphasize security, not sharing."[83] An allied official put it this way: "It's NOFORN, and it has always been that way."[84] The official went on to warn of the difficulty of change, noting that a sentiment of "this is the way we've always done it" governs most procedures.

Internally, all U.S. government agencies have significant punishments for sharing information improperly and few rewards for doing so well.[85] Indeed, punishment is often at the individual level: if a well-meaning junior official makes a sharing decision that is later deemed a mistake, the junior official is at risk of punishment and even (though rare) prosecution. ("The O-4 might not get cover," one foreign official put it.[86]) Indeed, the United States has a long history of aggressively prosecuting low-level leakers while being less aggressive toward senior officials when they leak.[87]

There are, however, potential work-arounds. Removing NOFORN designations can be done, but it is bureaucratically difficult for some agencies. The chairman of the Joint Chiefs of Staff, for example, can direct DIA to remove a NOFORN label on occasion, but

doing so on a routine basis is hard.[88] In general, when a request to downgrade highly classified information to a more releasable level is eventually approved, or when a "tearline"—which eliminates some information, giving an ally only a partial picture—is created, some useful information can be transmitted. This process, however, is often lengthy.[89]

Proliferation of Veto Players

U.S. intelligence sharing is governed by several guidelines. Most notable is Intelligence Community Directive 403, which covers "Foreign Disclosure and Release of Classified National Intelligence." Other guidelines deal with areas including more general classification and tearlines for intelligence sharing. Directive 403 declares, "It is the policy of the U.S. Government to share intelligence with foreign governments whenever it is consistent with U.S. law and clearly in the national interest to do so, and when it is intended for a specific purpose and generally limited in duration." The directive also notes that the intelligence community "shall limit the use of restrictive dissemination control markings to the minimum necessary."[90]

Although these guidelines offer a degree of consistency, they also illustrate several limits and potential problems. First, although ODNI provides overall guidance, it does not control or direct sharing with allies. The system is decentralized, and the intelligence community personnel representing the agencies from which the information originates are responsible for approving release to foreign governments, as these personnel are usually best placed to know the cost if the information and associated sources and methods were to be lost. Given the United States' numerous collection entities, there is often considerable variation in how guidance is interpreted. In addition, the guidance is unclear as to what role the intelligence community should play in building partner capacity to better enable sharing.

The problems within the Department of Defense, where half of the 18 U.S. intelligence entities reside, are particularly complex. DOD has its own policies for releasing classified information to foreign governments. These policies are opaque overall, leaving decisions up to various agencies or, at times, individual personnel. Often those tasked with foreign disclosure are analysts with minimal training and many other responsibilities. Even sharing with Five Eyes requires additional permissions.[91] As a result, per Corbett and Danoy, "The busy analyst is therefore more likely to opt for the safe option of defaulting to NOFORN."[92] Indeed, one foreign intelligence official wryly noted that information their service provided to the Five Eyes later received a NOFORN label.[93] Another noted that they have seen Controlled Unclassified Information (CUI) information show up as NOFORN.

Ironically, some post-9/11 measures to improve internal U.S. sharing have hindered sharing with foreign partners. After 9/11, there were efforts to bring various intelligence agencies together, such as the creation of more fusion cells. As a result, where once one agency might have allowed a cleared foreign official to be in the room or to read intelligence, now all agencies get a say; some invariably have stricter rules than others, resulting in a lowest-common-denominator effect.[94]

These problems vary depending on which U.S. agencies are involved. Often, collectors of the same type of intelligence (e.g., SIGINT) find it easier to share information with foreign partners than to do so domestically, due to cultural and technical system compatibilities.[95] The FBI, in contrast, faces steep difficulties in foreign sharing, a fact that hampers its potentially important role against Russian and Chinese subversion at the domestic level, among other things. Because FBI information concerns U.S. citizens, sharing is often difficult for legal and political reasons.[96]

The problem is often worse in the United States than outside of it, which demonstrates the importance of both bureaucratic compatibility and trust. U.S. and joint facilities outside the United States tend to have fewer bureaucratic players, "and they are more at the pointy end," as one foreign intelligence official put it. These countries are more aware of the risks of not sharing—the sense of which gets "diluted in the safety of D.C," in the words of one official—and more attuned to how information might be used.[97]

At times, the problems that result from overly vigilant security can lead to small indignities. Even Five Eyes–affiliated individuals embedded in U.S. agencies must often work in physically separate parts of offices, which further reduces intelligence sharing and decreases per-

sonal bonds.[98] According to one official, cleared foreign officials can escort guests from their own governments and militaries at DIA, NGA, and NSA, but not at the Pentagon. As a result, there is significant paperwork for both U.S. and foreign officials when allied officers and officials visit. In addition to wasting time, this state of affairs signals a lack of faith: "They don't trust us to go to the bathroom," sighed one official.[99]

The Cost of the Failure to Share

The cost of these problems is high. Measuring their direct impact, however, is difficult, as the counterfactual—what would improve with more sharing?—is impossible to gauge. As one former allied intelligence official put it, "It's hard to know what you don't know."[100]

At the very least, some valuable information fails to reach allies. One non-U.S. intelligence official noted that they rarely see U.S. information in their day-to-day work.[101] This, in turn, affects threat perceptions and attitudes toward the United States. Allies may prove slower to recognize aggression from Beijing, Moscow, or other revisionist powers in the absence of salient U.S. intelligence.

Cooperation is likely to suffer both before and during a crisis, even if more information is eventually shared. Allied military forces may have sub-optimal postures, fail to be prepared for a confrontation, or lack effective cooperation during a crisis: as one official put it, key figures may be exchanging business cards as they meet for the first time rather than rolling up their sleeves to work.[102]

A lack of intelligence sharing can mean that an important tool for building overall relationships is not being fully employed. Though it usually takes place behind the scenes, such sharing can help a relationship endure even as public relations become fraught.

The United States sets its own collection requirements, as do most allies; this can make resource issues more pronounced. Because collection is not coordinated, the United States often does not know what information allies—even Five Eyes countries—already have, thus reducing the economy of efforts.[103]

Timeliness is another problem. U.S. guidance calls for responses to sharing requests to be made within seven working days, a frame that only works if information is not time sensitive. As one U.S. official noted, "the [foreign disclosure officer] process can be a day, it can be a month." Much depends on the degree to which information must go back to originating agencies, and how many agencies are involved.[104]

The United States can and does alter how it shares intelligence when a crisis or other priority change occurs: U.S. sharing with Ukraine and other European countries, for example, increased significantly after the 2022 Russian invasion. This both improved threat assessments and operational coordination.[105]Allies are aware that such sharing can change dramatically, but the conditions under which this might occur are not always clear.[106] Future-oriented intelligence, including some long-term assessments, is often NOFORN.[107] One allied intelligence officer noted that their country enjoyed good cooperation with U.S. intelligence services during Operation Prosperity Guardian, which countered Houthi aggression in the Red Sea, but that such cooperation had been lacking before the crisis.[108] As one allied defense leader noted, "We seek both predictability and speed."[109]

Sharing information at the strategic level, although usually less immediate, is vital for long-term alignment. As one intelligence officer noted, "For our country to change its policies, we need intelligence at the policy level." The officer went on to note that this was particularly important because great power competition, unlike counterterrorism, involves more diffuse problems and many tradeoffs, all of which causes policies to be in flux.[110]

CHAPTER 04

Recommendations for Improving Intelligence Sharing

A pile of secret and classified documents released from the National Archives on March 23, 2004, in London.
IAN WALDIE/GETTY IMAGES

Changing the status quo by reducing barriers to intelligence sharing is an urgent task. However, many of the barriers to effective sharing cannot be changed or would be very difficult to alter. Varied interests are an inherent part of international relations, and the United States and its allies should not expect to always agree on the nature of threats and how to meet them. In addition, U.S. and allied cultures and political systems change slowly at best—and when they do, the drivers have little to do with intelligence sharing.

Significant progress can be made, however, if the United States is willing to take action to change its approach to sharing and bureaucratic procedures. The necessary steps are both difficult and painful, and many come with genuine tradeoffs. They are necessary, however, if the United States is to work more closely with allies and partners.

Prioritization and Diplomacy

The approach of "need to know" should be followed when applied with common sense, but it is currently used to justify overclassification. Some goals are worth the counterintelligence risk inherent in greater sharing; in other cases, it is worth denying potential partners information in the name of protecting sources and methods. One official noted that they were

constantly bombarded with requests for sharing by individuals who had little need to know. The intelligence office at the National Security Council should approach this prioritization via an interagency process and enforce it with various agencies, both in situations where more sharing is required and at times when it is not necessary.

Although this report focuses on U.S. problems, many of the sharing issues are on the partner side, and improved intelligence should also be a diplomatic priority. The United States should encourage allies to invest more in their intelligence services, improve their sharing internally, strengthen their counterintelligence, and upgrade their technical systems to ensure compatibility and security.

A Revamped Security Culture

Perhaps the biggest challenges to improved sharing involve revising security protocols and changing internal incentives. The skill of Chinese and Russian intelligence agencies makes this a difficult and evolving challenge. Revising security protocols will entail assuming more risk: The more intelligence shared with allies, the more likely adversaries are to gain access to secret information via leaks and security lapses, which can have costly consequences. The current approach, however, involves the opposite form of risk—a form that is harder to observe but likely more costly, as under sharing results in missed opportunities to improve U.S. and allied security. The personal connections, knowledge of allies' intelligence cultures and political realities, and other intangibles will grow if cooperation grows, further enhancing security. Indeed, one senior U.S. official noted that joint operations can build trust, which leads to better operations.[1] Better training would also make sharing more effective and would help change culture in the long term.

A culture shift of this magnitude will require allies to make security improvements, and the United States should encourage and at times help devote resources to these improvements. At the same time, imperfections in allies' intelligence systems should not be excuses for inaction. The United Kingdom was initially (and rightly) skeptical of U.S. security procedures at the onset of Five Eye cooperation after World War II and worked with the United States to improve its counterintelligence. The United Kingdom took a gamble in sharing information with the United States in the early days of the Cold War—but over time, a robust relationship developed that led to considerable trust. Australia, to give another example, has had to upgrade its facilities and counterintelligence to expand sharing with the United States.[2] Similarly, Japan has improved its counterintelligence to gain better access to sensitive U.S. equipment like satellite tracking.[3]

It is vital that the incentives for individuals involved in declassification are changed. This would involve increasing training, reducing the risk of individual punishment, and providing incentives for sharing. The risk for individuals of allowing a security breach is high, but there is little payoff for successful sharing.

Reducing NOFORN

Security fears have led to the NOFORN designation being used too frequently, according to this paper's interviewees, to the point that it is essentially the default rather than a deliberate decision. As one former U.S. intelligence official put it, the goal should be to go from NOFORN to "YESFORN": The default should be sharing, and collectors or security officers should have to prove that sharing should not occur, especially with Five Eyes and other highly trusted allies. This would considerably reduce the friction in the process.[4] Below are several useful steps that could be implemented to enable this.

- For Five Eyes representatives who work in U.S. intelligence agencies, the NOFORN caveat should be removed for nearly everything.
- ODNI and the Office of the Undersecretary of Defense for Intelligence and Security should have greater power to increase intelligence sharing across the agencies they coordinate and should push to make "Releasable to FVEY" a more common classification.[5]
- NOFORN should be removed from most finished intelligence for trusted partners after source ref-

erences are eliminated. As Corbett and Danoy note, "Finished intelligence, by definition, has been through a rigorous editing and approval process, and the chances of a serious disclosure breach are minimal."[6]

- Establishing procedures for automatic release if a formal decision is not forthcoming by a certain deadline. It is often bureaucratically easier to delay information releases and, even if the information is approved for sharing eventually, this delay reduces the information's value. These procedures would apply to NOFORN documents without significant additional codewords.

Expanding Low-Risk Sharing

Even as the United States considers changing its procedures, experimentation in more aggressive sharing should begin in low-risk areas. Corbett and Danoy suggest climate change as one area where information is both valuable and rarely highly classified.[7] With successful pilots in these areas, sharing could be expanded to more sensitive spheres.

As the use of AI expands, sharing via algorithm should also be explored—again, with low-risk areas as a starting point. Because the use of AI is steadily growing, it will be essential to understand the conditions under which AI can expedite sharing in order to improve future cooperation.

Open-source information (OSINT), which is increasing in quality and quantity, can usually be shared with ease.[8] Directing countries in which sharing is harder for security reasons—such as the Philippines and Taiwan—to reliable OSINT can provide a common threat picture at a basic level. For example, data from commercial satellites has helped the Quad (the United States, Australia, India, and Japan) track China's maritime smuggling and maritime militia. Unclassified information provided to India by the United States after the signing of the Basic Exchange Cooperation Agreement on Geospatial Intelligence in 2020 helped India repel a Chinese incursion along the contested border in the Himalayas.[9] Similarly, some aspects of space awareness are also unclassified.[10] The OSINT community should work to produce more finished intelligence on demand, which could then be incorporated easily into information shared with partners.

Advances in commercial technology will also require revisiting the sensitivity of classified collection and analysis. Commercial geospatial capabilities, for example, have improved dramatically in recent years, surpassing older systems whose capabilities were extraordinarily secret. This shift allows greater sharing of information in a realm that was once highly classified.

Resourcing and Personnel

In some agencies, it is often difficult for busy intelligence officers to declassify information in a timely way. This is particularly the case when analysts do not fully understand classification rules (some of which are contradictory) and the penalties for security violations are high. Allowing more foreign access would require some originating organizations to further develop their own disclosure expertise and clearance procedures, which would mean a significant resource investment.[11] This would require new foreign disclosure officers and similar personnel to receive more training. It would also require training for analysts and collectors to write products that both allow for greater sharing and protect sources.

Improving cooperation will also require helping partner governments improve their security, invest in new technology for information sharing systems, and take on more personnel to manage relationships. Buying more communications systems and ensuring compatibility will be expensive and will require major investments. The rewards usually outweigh the costs, however, especially over time and during crises.

Improved language skills will also be vital. U.S. intelligence agencies' problems with foreign languages are well documented.[12] It is not a coincidence that the most successful sharing alliance, the Five Eyes, involves a common language. The United States at times deploys military and intelligence officers to foreign agencies with the expectation that foreign personnel should operate in English.[13] "Imagine how much bet-

ter relations would be," one official commented, if U.S. officials could operate in allies' languages.[14]

Longer tours for liaison officers would be helpful. This could be difficult for hardship tours and, bureaucratically, could put intelligence officers out of sync with the State Department; however, it would greatly help build expertise and personal connections.[15]

Expanding the Circle

There have been many calls to expand the Five Eyes, with proposals for the inclusion of countries such as France, Germany, Japan, and South Korea, although a British report noted that "there is little prospect of expansion, at least in the medium term" due to the high levels of trust needed to enter this exclusive club.[16] These nations already have significant intelligence cooperation with the United States, as well as common interests. Germany has a strong space presence, proximity to Russia, careful SIGINT procedures, and even an embassy in Pyongyang that might allow greater access to North Korea. France also has a large space presence, excellent SIGINT, and a presence in Africa and South America through its overseas territories, including islands like Mayotte and Réunion. South Korea, of course, boasts impressive collection and analysis on North Korea, as well as access to information on China.[17] These countries would need to resolve their own balkanization problems and properly resource their services as conditions for significantly closer sharing.

Some countries that are ideal partners in efforts against China and Russia have significant security problems, limiting cooperation. India is a useful strategic partner, but it has numerous ties to Russia. Taiwan, while useful, is a place where China has an extensive intelligence presence.[18]

A valuable alternative to expanding the Five Eyes, especially given the high trust barrier, would be to develop smaller alternative groups that are focused on particular targets and on sharing a narrow scope of information. For example, the United States has expanded intelligence liaison relationships with Quad countries.[19] A China-focused group would be an obvious step and could consist of existing Five Eyes partners like Australia and New Zealand, with additions like Japan and South Korea; Taiwan and the Philippines could also play roles, albeit lesser ones, given their security weaknesses. There is danger, however, in forming clubs, which creates new haves and have-nots, potentially generating resentment and reducing trust. Nevertheless, alliances can also create incentives for the improvement of security procedures, the forming of common protocols, and so on.[20]

When expanding circles of intelligence sharing, there will inevitably be mistakes—possibly grievous ones. As it is, however, the United States is paying the cost of insufficient sharing on a daily basis.

Conclusion

Intelligence sharing, while fraught with challenges, is indispensable to enhancing U.S. security. The imperfections of intelligence sharing demand an aggressive approach to reform. The United States must foster a more agile and inclusive environment for intelligence collaboration. This endeavor should not merely be about refining tactics or expanding networks, but about strategically rethinking the foundational aspects of security collaboration to better address the threats of today and tomorrow. By taking on this challenge, the United States and its allies can enhance their strategic foresight, operational efficiency, and collective response capabilities, ultimately ensuring improved security for all participants.

About the Author

Daniel Byman is the director of the Warfare, Irregular Threats, and Terrorism Program at the Center for Strategic and International Studies (CSIS). He is also a professor at Georgetown University's School of Foreign Service and director of the Security Studies Program. He is the foreign policy editor for *Lawfare* and a part-time senior adviser to the Department of State on the International Security Advisory Board. In addition to serving as the vice dean for the School of Foreign Service at Georgetown, he was a senior fellow at the Center for Middle East Policy at the Brookings Institution and a professional staff member with both the National Commission on Terrorist Attacks on the United States (9-11 Commission) and the Joint 9/11 Inquiry Staff of the House and Senate Intelligence Committees. He formerly served as research director of the Center for Middle East Public Policy at the RAND Corporation and as a Middle East analyst for the U.S. intelligence community. Dr. Byman is a leading researcher and has written widely on a range of topics related to terrorism, insurgency, intelligence, social media, artificial intelligence, and the Middle East. He is the author of nine books, including *Road Warriors: Foreign Fighters in the Armies of Jihad* (Oxford, 2019), *Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs Know* (Oxford, 2015), and *A High Price: The Triumphs and Failures of Israeli Counterterrorism* (Oxford, 2011). He is the author or coauthor of almost 200 academic and policy articles, monographs, and book chapters as well as numerous opinion pieces in the *New York Times*, *Wall Street Journal*, *Washington Post*, and other leading journals. Dr. Byman is a graduate of Amherst College and received his PhD in political science from the Massachusetts Institute of Technology.

Endnotes

EXECUTIVE SUMMARY

1 Mark Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: Congressional Quarterly Press, 2003), 8.

2 Sean Corbett and James Danoy, "Beyond NOFORN: Solutions for Increased Intelligence Sharing among Allies," Atlantic Council, *Issue Briefs*, October 31, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/.

3 This paper emphasizes concerns about Russia and especially China, with less focus on the Middle East. I believe, however, that most of the findings are relevant to efforts against Iran and other potential adversaries in that region.

4 Richard J. Aldrich, "Transatlantic Intelligence and Security Cooperation," *International Affairs* 80, no. 4 (2004): 731–753, https://www.jstor.org/stable/3569532.

CHAPTER 1: THE IMPORTANCE OF INTELLIGENCE SHARING

1 Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 527–542, https://www.tandfonline.com/doi/abs/10.1080/716100467; H. Bradford Westerfield, "America and the World of Intelligence Liaison," *Intelligence and National Security* 11, no. 3 (1996): 529, https://doi.org/10.1080/02684529608432375.

2 Intelligence and Security Committee of Parliament, *International Partnerships* (London: December 2023), section 1, https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-International-Partnerships.pdf.

3 Jennifer E. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and CounterIntelligence* 19, no. 2 (2006): 195–217, https://doi.org/10.1080/08850600500483657.

4 Interview with U.S. senior official, September 30, 2024.

5 Interview with senior U.S. official, August 11, 2024; and interview with U.S. senior official, September 30, 2024.

6 Intelligence and Security Committee of Parliament, *International Partnerships*, section 49.

7 Interview with non-U.S. expert, December 13, 2024.

8 Daniel Byman, "The Intelligence War on Terrorism," *Intelligence and National Security* 29, no. 6 (2014): 837–863, https://doi.org/10.1080/02684527.2013.851876; Bruce Hoffman, Edwin Meese III, and Timothy J. Roemer, *The FBI: Protecting the Homeland in the 21st Century* (Washington, DC: 9/11 Review Commission, March 2015), https://www.fbi.gov/file-repository/final-9-11-review-commission-report-unclassified.pdf/view.

9 Artur Gruszczak, "The Polish Intelligence Services," in *Geheimdienste in Europa: Transformation, Kooperation und Kontrolle*, ed. T. Jäger and A. Daun (Wiesbaden, Germany: VS Verlag für, 2009), 145.

10 Park Si-soo, "U.S., South Korea Agree to Cooperate on Space Situational Awareness for Military Purposes," SpaceNews, August 26, 2002, https://spacenews.com/u-s-south-korea-agree-to-cooperate-on-space-situational-awareness-for-military-purposes/.

11 Adam D.M. Svendsen, "The Globalization of Intelligence Since 9/11: The Optimization of Intelligence Liaison Arrangements," *International Journal of Intelligence and CounterIntelligence* 21, no. 4 (2008): 664, https://doi.org/10.1080/08850600802254871.

12 Interview with non-U.S. expert, December 13, 2024.

13 Interview with non-U.S. expert, October 8, 2024.

14 Stephen Lander, "International Intelligence Co-operation: An Inside Perspective," *Cambridge Review of International Affairs* 17, no. 3 (October 2004): 482, https://doi.org/10.1093/acrefore/9780190846626.013.222.

15 Interview with non-U.S. expert, October 3, 2024.

16 Aldrich, "Transatlantic Intelligence," 749.

17 Svendsen, "The Globalization of Intelligence."

18 Byman, "The Intelligence War"; and Anthony R. Wells, *Between Five Eyes: 50 Years of Intelligence Sharing* (Havertown: Casemate Publishers, 2020), 89.

19 David R. Shedd, *The Intelligence Posture America Needs in an Age of Great-Power Competition* (Washington, DC: The Heritage Foundation, November 2020), 71, https://www.heritage.org/military-strength-topical-essays/2021-essays/the-intelligence-posture-america-needs-age-great-power.

20 The focus of this paper is on great power competition, but many of the findings and recommendations would apply to work with allies against Iran and other regional adversaries.

21 Peter Martin and Jenny Leonard, "U.S. Weaves Web of Intelligence Partnerships Across Asia to Counter China," Bloomberg, October 5, 2023, https://time.com/6320722/us-asia-intelligence-partnerships-china/.

22 "Russian Spies Are Back—and More Dangerous than Ever," *The Economist*, February 20, 2024, https://www.economist.com/international/2024/02/20/russian-spies-are-back-and-more-dangerous-than-ever; U.S.-China Economic and Security Review Commission, *China's Intelligence Services and Espionage Threats to the United States* (Washington, DC: U.S. Government Publishing Office, 2019), https://www.uscc.gov/sites/default/files/2019-11/Chapter%202%2C%20Section%203%20-%20China%27s%20Intelligence%20Services%20and%20Espionage%20Threats%20to%20the%20United%20States.pdf.

23 Alan W. Throop and Sam Fairall-Lee, "US-Australia Information Sharing: A Self-Inflicted Achilles' Heel," Australian Strategic Policy Institute, November 10, 2022, https://www.aspistrategist.org.au/us-australia-information-sharing-a-self-inflicted-achilles-heel/.

24 Interview with foreign government official, September 26, 2024.

CHAPTER 2: INTELLIGENCE SHARING STRUCTURES

1 Westerfield, "America and the World."

2 Lefebvre, "The Difficulties," 533.

3 Interview with senior U.S. official, August 11, 2024.

4 Sims, "Foreign Intelligence," 197.

5 Jeffrey T. Richelson, "The Calculus of Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence* 4, no. 3 (1990): 315, https://doi.org/10.1080/08850609008435147.

6 Kiyoung Chang, "'I Know Something You Don't Know': The Asymmetry of 'Strategic Intelligence' and the Great Perils of Asymmetric Alliances," *British Journal of Politics and International Relations* 25, no. 3 (2023): 480–497, https://journals.sagepub.com/doi/10.1177/13691481221109727."

7 Judy Dempsey, "NATO's Intelligence Deficit: It's the Members, Stupid!" Carnegie Endowment for International Peace, *Commentary*, May 25, 2017, https://carnegieendowment.org/europe/strategic-europe/2017/05/natos-intelligence-deficit-its-the-members-stupid?lang=en&center=europe; Joseph S. Gordon, "Intelligence Sharing in NATO," *Atlantisch Perspectief* 41, no. 6 (2017): 15–19, https://www.jstor.org/stable/48581386 (Similar

arguments are made regarding intelligence sharing in the Visegrad Group); Šárka Kolmašová, "Competing Norms and Strategic Visions: A Critical Appraisal of V4 Security Potential," *Europe-Asia Studies* 71, no. 2 (2019): 225–48, https://doi.org/10.1080/09668136.2018.1562045; and Carleigh A. Cartmell, "Long Term Intelligence Sharing: The Five Eyes and the European Union," *Journal of Intelligence History* 22, no. 3 (2023): 417–34, https://doi.org/10.1080/16161262.2022.2085940.

8 Sims, "Foreign Intelligence," 202.

9 John Battersby and Rhys Ball, "The Phantom Eye: New Zealand and the Five Eyes," *Intelligence and National Security* 38, no. 6 (2023): 920, https://doi.org/10.1080/02684527.2023.2212557.

10 Corey Pfluke, "A History of the Five Eyes Alliance: Possibility for Reform and Additions," *Comparative Strategy* 38, no. 4 (2019): 303, https://doi.org/10.1080/01495933.2019.1633186; and Battersby and Ball, "The Phantom Eye," 920.

11 Stephen Lander, "International Intelligence Co-operation: An Inside Perspective," *Cambridge Review of International Affairs* 17, no. 3 (October 2004): 487.

12 Westerfield, "America and the World," 529; and Lander, "International Intelligence," 491–492.

13 Pfluke, "A History," 305–306.

14 Pfluke, "A History," 305–306.

15 Intelligence and Security Committee of Parliament, *International Partnerships*, section 200.

16 Westerfield, "America and the World," 529; Lander, "International Intelligence," 491–492; and Intelligence and Security Committee of Parliament, *International Partnerships*, section 184.

17 Intelligence and Security Committee of Parliament, *International Partnerships*, section 201.

18 Lander, "International Intelligence," 487; John Blaxland and Clare Birgin, *Revealing Secrets: An Unofficial History of Australian Signals Intelligence & the Advent of Cyber* (Sydney: University of New South Wales Press, 2023), 226.

19 Wells, *Between Five Eyes*, 107.

20 Interview with former senior U.S. official, November 5, 2024.

21 Michael S. Goodman, "The Foundations of Anglo-American Intelligence Sharing," *Studies in Intelligence* 59, no. 2 (2015) 4–6, https://www.cia.gov/resources/csi/static/Foundations-of-Anglo-American.pdf.

22 Blaxland and Birgin, *Revealing Secrets*, 208–209.

23 Goodman, "The Foundation," 7.

24 Interview with former senior U.S. official, October 21, 2024.

25 Battersby and Ball, "The Phantom Eye," 921.

26 Interview with former senior U.S. official, October 21, 2024.

27 "Denmark is One of NSA's '9-Eyes'," *Copenhagen Post*, November 4, 2013, https://cphpost.dk/2013-11-04/general/denmark-is-one-of-the-nsas-9-eyes/.

28 Jonathan Panter, "Missile Defense: How Vulnerable Is Israel to Iran's Attacks?", Council on Foreign Relations, Expert Brief, October 16, 2024, https://www.cfr.org/expert-brief/missile-defense-how-vulnerable-israel-irans-attacks.

29 Scott W. Harold, "South Korea Should Consider Sticking with Intelligence-Sharing Pact with Japan," RAND, *Commentary*, November 5, 2019, https://www.rand.org/pubs/commentary/2019/11/south-korea-should-consider-sticking-with-intelligence.html; and

Yusuke Takeuchi and Junnosuke Kobara, "U.S., Japan, South Korea Start Sharing Missile Information in Real Time," *Nikkei Asia*, December 20, 2023, https://asia.nikkei.com/Politics/Defense/U.S.-Japan-South-Korea-start-sharing-missile-information-in-real-time.

30 Interview with non-U.S. intelligence official, August 12, 2024.

31 Interview with foreign government official, May 9, 2024; and interview with non-U.S. official, October 19, 2024.

32 Lefebvre, "The Difficulties," 534.

CHAPTER 3: COMMON INTELLIGENCE COOPERATION PROBLEMS

1 Hyesoo Seo, "Intelligence Politicization in the Republic of Korea: Implications for Reform," *International Journal of Intelligence and CounterIntelligence* 31, no. 3 (2018): 453, https://doi.org/10.1080/08850607.2018.1466566; Youngshik Daniel Bong, "The US-South Korea Alliance: Local, Regional, and Global Dimensions," *Asian Politics & Policy* 8, no. 1 (2016): 41, https://doi.org/10.1111/aspp.12242.

2 Interview with non-U.S. expert, October 3, 2024.

3 Interview with non-U.S. expert, October 8, 2024.

4 Justin Lynch, "In the Intelligence Business, Friends are Hard to Come By," New America Foundation, March 19, 2015, https://www.newamerica.org/weekly/intelligence-business-friends-are-hard-come/.

5 Interview with foreign government official, May 9, 2024.

6 Radek Sikorski, "Don't Take Poland for Granted," *Washington Post*, March 21, 2007, https://www.washingtonpost.com/archive/opinions/2007/03/21/dont-take-poland-for-granted/163c70e9-4ee3-40fb-8ed3-980ebe0ad86a/.

7 Interview with non-U.S. expert, October 3, 2024.

8 Interview with non-U.S. expert, October 7, 2024.

9 Interview with non-U.S. official, October 19, 2024.

10 Interview with former non-U.S. official, October 21, 2024.

11 Interview with non-U.S. officials, October 7, 2024.

12 Interview with non-U.S. expert, September 19, 2024.

13 Interview with foreign government officials, August 19, 2024.

14 Bong, "The U.S.-South Korea," 45; interview with foreign government official, May 9, 2024; and interview with former non-U.S. official, October 21, 2024.

15 Interview with non-U.S. expert, September 19, 2024.

16 Daniel R. Depetris, "Bridging the Divide: The Significance of the US-South Korea-Japan Trilateral," Lowy Institute, *The Interpreter*, August 17, 2023, https://www.lowyinstitute.org/the-interpreter/bridging-divide-significance-us-south-korea-japan-trilateral.

17 Interview with U.S. senior official, September 30, 2024.

18 Interview with non-U.S. expert, October 8, 2024; and interview with former senior U.S. official, October 21, 2024.

19 Interview with non-U.S. expert, October 3, 2024.

20 Interview with non-U.S. expert, September 19, 2024.

21 Chang, "'I Know'," 481.

22 Ibid., 489; and K. Lee, "The US was Aware of the Infiltration of Armed Spies," *Sisa Journal*, October 17, 1996, https://www.sisajournal.com/news/articleView.html?idxno=78420.

23 Chad De Guzman, "Leaked Pentagon Documents Appear to Show U.S. Spying on Ally

South Korea," *Time*, April 10, 2023, https://time.com/6269905/us-pentagon-leaked-documents-south-korea/; Martin and Leonard, "U.S. Weaves Web"; and interview with non-U.S. expert, September 19, 2024.

24 Westerfield, "America and the World," 539.

25 Interview with non-U.S. expert, September 19, 2024.

26 Interview with non-U.S. officials, October 7, 2024.

27 In the United States, this imbalance can lead to concerns about burden sharing, an especially sensitive issue for political leaders like Donald Trump.

28 Lander, "International Intelligence," 486.

29 Andrew O'Neil, "Australia and the 'Five Eyes' Intelligence Network: The Perils of an Asymmetric Alliance," *Australian Journal of International Affairs* 71, no. 5 (2017): 531, https://doi.org/10.1080/10357718.2017.1342763.

30 Chang, "'I Know'," 487.

31 Interview with non-U.S. intelligence official, August 12, 2024.

32 Chang, "'I Know'," 492; and interview with former non-U.S. official, October 21, 2024.

33 O'Neil, "Australia and the 'Five Eyes'," 538; Mike Scrafton, "Abandoned Sovereignty: Australia's Intelligence Function Colonised by US," *The Mandarin*, August 7, 2023, https://www.themandarin.com.au/227244-australias-intelligence-function-colonised-by-us/; Ben Scott, "Five Eyes: Blurring the Lines between Intelligence and Policy," Lowy Institute, July 27, 2020, https://www.lowyinstitute.org/the-interpreter/five-eyes-blurring-lines-between-intelligence-policy; and Geoffrey Barker, *Sexing It Up: Iraq, Intelligence and Australia* (Sydney: University of New South Wales Press, 2003), 17.

34 Blaxland and Birgin, *Revealing Secrets*, 219.

35 Gruszczak, "The Polish Intelligence," 140–141.

36 Interview with non-U.S. officials, August 29, 2024.

37 Interview with non-U.S. expert, September 19, 2024.

38 Gruszczak, "The Polish Intelligence," 148; and interview with non-U.S. expert, October 3, 2024.

39 Intelligence and Security Committee of Parliament, *International Partnerships*, section 210.

40 Sims, "Foreign Intelligence," 202.

41 Pfluke, "A History," 307.

42 Interview with non-U.S. expert, October 8, 2024.

43 Blaxland and Birgin, *Revealing Secrets*, 339.

44 Interview with foreign government official, September 26, 2024.

45 Interview with senior U.S. official, August 11, 2024.

46 Lefebvre, "The Difficulties," 535.

47 Svendsen, "The Globalization," 664.

48 Interview with U.S. official, October 7, 2024.

49 Ben Blanchard and Roger Tung, "Taiwan Drills to Focus on Piercing Blockade, Get 'Five Eyes' Intelligence Link," Reuters, August 26, 2023, https://www.reuters.com/world/asia-pacific/taiwan-war-games-focus-combating-blockade-preserving-forces-2023-04-26/.

50 Interview with non-U.S. officials, October 7, 2024.

51 Interview with non-U.S. officials, August 29, 2024.

52 Interview with U.S. official, November 3, 2024.

53 Interview with non-U.S. officials, October 7, 2024.

54 Interview with U.S. official, November 3, 2024.

55 Interview with non-U.S. officials, August 29, 2024.

56 Interview with foreign government official, September 26, 2024.

57 Interview with senior U.S. official, August 11, 2024.

58 Interview with U.S. official, October 7, 2024.

59 Interview with U.S. official, November 3, 2024.

60 Corbett and Danoy, "Beyond NOFORN."

61 Interview with U.S. official, November 3, 2024.

62 Interview with senior U.S. official, August 11, 2024.

63 Cho Sunghwan, "A Comparative Study on Information Sharing of National Security Agencies: Case Analysis of Information Sharing in the Republic of Korea's National Security Agencies and the U.S. Intelligence Community" (PhD diss., Kyunggi University, 2016).

64 Svendsen, "The Globalization of Intelligence," 671.

65 Richard J. Aldrich, "International Intelligence Cooperation in Practice," in *International Intelligence Cooperation and Accountability*, ed. Hans Born, Ian Leigh, and Aidan Wills (Routledge, 2011), 26, https://api.pageplace.de/preview/DT0400.9781136831409_A24325249/preview-9781136831409_A24325249.pdf.

66 Interview with non-U.S. intelligence official, August 12, 2024; and interview with U.S. official, October 7, 2024.

67 Gruszczak, "The Polish Intelligence," 126.

68 Interview with senior U.S. official, August 11, 2024.

69 David Rosenberg, "Pine Gap: An Historical Perspective on Australia's Intelligence-Sharing Partnership with the United States in a Time of Political Change," *United Service* 70, no. 3 (2019): 14; and Blaxland and Birgin, *Revealing Secrets*, 275–279.

70 Interview with foreign government officials, August 19, 2024.

71 Lander, "International Intelligence," 487.

72 Seo, "Intelligence Politicization," 456.

73 Ibid., 462.

74 Gruszczak, "The Polish Intelligence," 130-131, 141, 148..

75 Lander, "International Intelligence," 493.

76 James J. Wirtz, "Constraints on Intelligence Collaboration: The Domestic Dimensions," *International Journal of Intelligence and CounterIntelligence* 6, no. 1 (1993): 87, https://doi.org/10.1080/08850609308435203.

77 Quoted in Corbett and Danoy, "Beyond NOFORN."

78 Ibid.

79 Interview with U.S. senior official, September 30, 2024.

80 Matthew Connelly, *The Declassification Engine: What History Reveals about America's Top Secrets* (New York: Vintage, 2024).

81 Patrick Radden Keefe, "The Cult of Secrecy," *Foreign Affairs*, February 13, 2023, https://www.foreignaffairs.com/reviews/patrick-radden-keefe-cult-of-secrecy-america-classification-crisis.

82 Interview with non-U.S. officials, October 7, 2024.

83 Interview with foreign government official, September 26, 2024.

84 Interview with non-U.S. officials, October 7, 2024.

85 Corbett and Danoy, "Beyond NOFORN."

86 Interview with foreign government official, September 26, 2024.

87 Keefe, "The Cult."

88 Interview with U.S. official, October 7, 2024.

89 Corbett and Danoy, "Beyond NOFORN."

90 "Intelligence Community Directive 403: Foreign Disclosure and Release of Classified National Intelligence," Office of the Director of National Intelligence, March 13, 2013, https://www.dni.gov/files/documents/ICD/ICD-403.pdf; "Intelligence Community Directive 209: Tearline Production and Dissemination," Office of the Director of National Intelligence, September 6, 2012, https://www.dni.gov/files/documents/ICD/ICD-209-Tearline-Production-and-Dissemination.pdf; and "Intelligence Community Directive 710: Classification Management and Control Marking Systems," Office of the Director of National Intelligence, June 21, 2013, https://www.dni.gov/files/documents/ICD/ICD-710.pdf.

91 Interview with foreign government official, September 26, 2024.

92 Corbett and Danoy, "Beyond NOFORN."

93 Interview with non-U.S. officials, August 29, 2024.

94 Interview with foreign government official, September 26, 2024.

95 Corbett and Danoy, "Beyond NOFORN."

96 Aldrich, "Transatlantic Intelligence," 740-41.

97 Interview with foreign government official, September 26, 2024.

98 Corbett and Danoy, "Beyond NOFORN."

99 Interview with foreign government official, September 26, 2024.

100 Interview with non-U.S. expert, October 8, 2024.

101 Interview with non-U.S. intelligence official, August 12, 2024.

102 Interview with former senior U.S. official, October 21, 2024.

103 Corbett and Danoy, "Beyond NOFORN."

104 Interview with non-U.S. officials, October 7, 2024.

105 Interview with former senior non-U.S. official, December 12, 2024.

106 Interview with U.S. official, October 7, 2024; Interview with non-U.S. officials, August 29, 2024.

107 Interview with non-U.S. officials, October 7, 2024.

108 Ibid.

109 Interview with non-U.S. officials, May 28, 2024.

110 Interview with non-U.S. officials, October 7, 2024.

CHAPTER 4: RECOMMENDATIONS FOR IMPROVING INTELLIGENCE SHARING

1 Interview with former U.S. official, November 5, 2024.

2 Svendsen, "The Globalization," 667; Blaxland and Birgin, *Revealing Secrets*, 260.

3 Martin and Leonard, "U.S. Weaves."

4 Interview with senior U.S. official, August 11, 2024.

5 Corbett and Danoy, “Beyond NOFORN.”

6 Ibid.

7 Ibid.

8 Ibid.

9 Martin and Leonard, “U.S. Weaves”; and Paul D. Shinkman, “U.S. Intel Helped India Rout China in 2022 Border Clash,” *U.S. News and World Report*, March 20, 2023, https://www.usnews.com/news/world-report/articles/2023-03-20/u-s-intel-helped-india-rout-china-in-2022-border-clash-sources.

10 Interview with non-U.S. officials, August 29, 2024.

11 Corbett and Danoy, “Beyond NOFORN.”

12 Beth J. Asch and John D. Winkler, *Ensuring Language Capability in the Intelligence Community* (Santa Monica, CA: RAND, 2013), https://www.rand.org/content/dam/rand/pubs/technical_reports/TR1200/TR1284/RAND_TR1284.pdf.

13 Interview with foreign government officials, August 19, 2024.

14 Interview with U.S. senior official, September 30, 2024.

15 Interview with senior U.S. official, August 11, 2024.

16 Intelligence and Security Committee of Parliament, *International Partnerships*, section 284.

17 Pfluke, “A History,” 309–312.

18 Interview with senior U.S. official, August 11, 2024.

19 Martin and Leonard, “U.S. Weaves.”

20 Interview with U.S. official, October 7, 2024; and Corbett and Danoy, “Beyond NOFORN.”

COVER PHOTO YAUHENKA/ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**