The Case for Cooperation
The Future of the U.S.-UK Intelligence Alliance

By Jake Harrington and Riley McCabe

THE ISSUE
Over the past 75 years, the United States and the United Kingdom have built the deepest intelligence alliance in the world. Despite decades of cooperation, however, there exists today a significant misalignment between the strategic prioritization of this “special relationship” and the regulations, policies, organizational cultures, and technologies that facilitate its day-to-day activities. This report’s recommendations are designed to encourage the adoption of policies, procedures, and tools that will enable the United States and the United Kingdom to achieve the deep level of collaboration they have repeatedly committed to in bilateral agreements, national security strategies, and intelligence guidance. If allies and partners are an indispensable pillar of both nations’ strategies to challenge rising and revanchist authoritarianism and other threats, then the U.S. and UK intelligence communities should jointly pursue robust interoperability that appropriately balances risk with opportunity.

To stay secret, we are going to have to become more open.

Achieving the goal captured in MI6 chief Moore’s remark will prove to be the greatest intelligence challenge of the twenty-first century. Today, technology, data, and information are profoundly disrupting the intelligence mission. Intelligence leaders in the United States and the United Kingdom rightly recognize that managing the complexity of the current security landscape requires them to emerge from the shadows. No intelligence service can navigate these challenges alone. Becoming more open is ultimately a call for strengthening and expanding partnerships and alliances.

Over the past 75 years, the United States and the United Kingdom have built the deepest intelligence alliance in the history of the Western world. It was forged in the common fight against Hitler’s fascism, fortified throughout the existential confrontation with Soviet communism, and sharpened during the global campaign against terrorism.

Today, the alliance is once again being mobilized to counter the threat of rising and revanchist authoritarianism. The United States and the United Kingdom face a common threat in Russia, which brazenly executes targeted assassinations on British soil, conducts global cyber and disinformation campaigns, and seeks to weaken Western institutions and alliances. Putin’s maximalist views of Russian power and his February 2022 decision to invade Ukraine pose the greatest threat to European security since World War II. Washington and London must also manage the prospect of a nuclear-capable Iran and potential further destabilization of the Middle East. And with respect to China, British and American concerns are increasingly converging. Both countries must grapple with Beijing’s military modernization, its development of repressive surveillance technologies, and its efforts to suppress freedom of expression both within its borders and abroad.
As Washington increasingly refers to China as the “pacing threat,” Chief Moore recently noted that “adapting to a world affected by the rise of China is the single greatest priority for MI6.” Moreover, these trends are all playing out against a backdrop of global democratic backsliding where, in the words of the U.S. Interim National Security Strategic Guidance, “democracies across the globe, including our own, are increasingly under siege.” For its own part, the United Kingdom’s Integrated Review argues that promoting democracy and an open, resilient, and rules-based international order is essential to meeting current and future threats.

U.S. and UK intelligence officers will have to navigate these shared threats together. In doing so, they will also have to overcome an array of common operational challenges. These include managing increasing volumes of data, both open-source and classified, that are impossible for any single analyst, agency, or country to handle on its own. This data crisis is fueling broader competition in the areas of artificial intelligence (AI), cloud computing, and quantum computing—all essential capabilities for conducting successful intelligence activities in the future. At the same time, both countries must also contend with how technology is disrupting traditional intelligence activities, particularly human intelligence operations. Commonly referred to as ubiquitous technical surveillance (UTS), the proliferation of cell phones, social media, biometrics, and smart city technologies are introducing profound questions about the future of cover. Just as allied signals intelligence agencies—first under the 1946 British-U.S. Communication Intelligence Agreement (UKUSA) and then in the expanded Five Eyes alliance—jointly navigated the complexities of the telecommunications age to develop innovative technologies and accesses throughout the Cold War, the human intelligence alliance will have to partner closely to develop effective tradecraft and doctrine to navigate the post-secrecy world.

Building on its ongoing work to assess the future of intelligence, the Center for Strategic and International Studies (CSIS), in partnership with the Royal United Services Institute (RUSI), undertook a 10-month project to assess the next era of the U.S.-UK intelligence alliance. CSIS and RUSI conducted research interviews with approximately 40 individuals in the United States and the United Kingdom with expertise across the areas of intelligence, technology, and transatlantic security. CSIS and RUSI also convened a structured workshop in October 2021 to review preliminary findings and recommendations with a similarly diverse range of experts.

This report is the culmination of those efforts. It proposes a set of priorities that the U.S. and UK intelligence communities should jointly pursue to enable robust, rapid, and scalable collaboration. These efforts are designed around a broad conception of interoperability. This includes traditional, technological notions of interoperability, such as shared approaches to system architecture, software, and data management. It also extends to reforming policy, guidance, bilateral agreements, and legal frameworks to make collaboration as seamless as possible. This report’s recommendations are designed to encourage the adoption of policies, procedures, and tools that enable the United States and the United Kingdom to achieve the deep level of collaboration they have repeatedly committed to in bilateral agreements, national security strategies, and intelligence guidance. If allies and partners are an indispensable pillar of both nations’ strategies to challenge rising authoritarianism and other threats, then the U.S. and UK intelligence communities should deepen integration in ways that appropriately balance risk with opportunity.

While addressing the barriers that constrain, delay, or impede intelligence collaboration that is beneficial to both nations, the proposed recommendations are also intended to preserve the sovereign prerogatives of each government. That is, when both countries agree that it is in their interest to collaborate, clear paths to success should be in place to enable a wide range of shared activities. Whether at a remote outpost, within a specific multilateral operation, or in support of broader collection and analysis, this report promotes simpler, streamlined, and predictable paths to collaboration.

**BUILDING AN ALLIANCE FOR THE FUTURE**

International intelligence collaboration is ultimately about expanding a service’s access to collection, analysis, technology, tradecraft, or training at lower costs than if they unilaterally attempted to replicate these activities. Intelligence scholar Jennifer Sims has aptly described this type of cooperation as “a form of subcontracted intelligence collection based on barter,” wherein intelligence information, access, or expertise is the currency. This transactional approach to intelligence liaison enables both sides of the partnership to leverage their comparative strengths, such as geographical, political, and technological advantages, to the mutual benefit of both parties.
MAKING INTELLIGENCE WORK FOR DEMOCRACY

Recent years have witnessed Russia, China, and other autocratic states adopt mass profiling and surveillance systems, relentlessly suppress free speech, criminalize political opposition, and propagate disinformation at home and abroad. Increasingly, the technologies that empower these actions are being exported and overlaid with narratives rejecting any suggestion that such behavior meaningfully deviates from that of the West. They lament that all criticism is rank hypocrisy in light of American, British, or other Western sins.

When democracy is under siege, its participants are the target. In the face of efforts to weaken confidence in democratic norms, values, and institutions, democracies must publicly articulate what they stand for. Countering narratives that seek to diminish the benefits of a transparent and free society is a crucial element of the emerging era of international competition. Although confronting ascendant and emboldened authoritarianism is not a challenge exclusive to intelligence, the U.S. and UK intelligence communities are being called upon to serve an indispensable role. The U.S.-UK intelligence alliance should aspire to serve as a model for how intelligence activities can and should be performed in democratic societies.

Core tenets of intelligence in a free society include building a cadre of professional intelligence officers who collect intelligence information consistent with human rights and international law; deliver objective, undistorted analysis to decisionmakers; refrain from intervening in policy deliberations or domestic politics; and respond to independent and transparent oversight. Intelligence agencies, even in democratic societies, are often granted extraordinary powers to protect a nation from harm. A healthy intelligence enterprise in a free society must strike an increasingly delicate balance between the national security imperative of secrecy and democracy’s need for transparency.

Promising work is underway in this area, and it should be sustained and amplified. Five Eyes intelligence leaders are making more frequent public appearances, often speaking in defense of democratic norms and values. Similarly, American and British intelligence services have made concerted efforts to increase public attribution of actors involved in recent disinformation, cyber, and military incidents. The Organization for Economic Cooperation and Development (OECD) also announced in late 2020 an initiative to promulgate a set of norms and best practices for how OECD member states should govern intelligence and law enforcement access to private data.

To the extent that liberal democracies are under siege, demonstrating that intelligence can be conducted in ways that advance—rather than undermine—civil liberties, human rights, and democratic values is crucial to the broader endurance of these beliefs. The ways that competitors like China and Russia advance visions of digital authoritarianism and abuse the tools of the security apparatus to control, intimidate, and punish their own people bring into stark focus the stakes of competing visions for the future of intelligence.

This report is not naïve enough to suggest that the U.S.-UK relationship entirely transcends the transactional theory of foreign liaison. There are no free rides in intelligence, at least not forever. However, the special relationship has indeed earned its title. Building an intelligence alliance as close as the one that exists between the United States and the United Kingdom requires hard work and immense trust. Joint operations double the risk of breaches, and differences between two services may increase confusion or spur disagreement. Nonetheless, the U.S.-UK intelligence alliance has survived even the darkest of hours, relying on a foundation of a kindred history and language, aligned strategic interests, and shared values.

Inefficiencies in how allies share intelligence information, including between the United States and the United Kingdom, have long been factored as a cost of doing business. All agencies and disciplines grapple with this issue, and still these barriers have not undercut the willingness of individual leaders or officers to develop joint operations or conduct bilateral analysis. In short, the problem is not the willpower of people. It is often while navigating technical, legal, and regulatory obstacles that individuals’ aspirations collide with reality.

Information and technology sharing between intelligence allies is guided by a combination of interconnected frameworks, policies, and protocols. These are intended
to balance commitments across a complex array of often overlapping frameworks, including legal; counterintelligence; personnel, physical, and information security; and privacy and civil liberties considerations. Intelligence is expensive and perishable, with the lives of human sources and costly technical accesses often in the balance. When catastrophic losses occur, security weaknesses are evaluated and additional countermeasures implemented. These procedures are well-intentioned, seeking to manage risk across all threat vectors, including foreign intelligence services, malicious cyber actors, insider threats, and terrorists. They govern how information technology systems are purchased, built, and secured; how personnel, partners, and vendors are screened for potential risks; and how information can be shared between agencies and with foreign partners.

GCHQ AND NSA: THE SPECIAL RELATIONSHIP WITHIN THE SPECIAL RELATIONSHIP

In 1946, the British-U.S. Communication Intelligence Agreement—commonly known as UKUSA—established a comprehensive agreement for the exchange of signals intelligence collection, cryptanalysis techniques, decryption and translation information, and analysis of various capabilities, practices, procedures, and equipment. This study confirms that there continues to exist what could be characterized as a “special relationship within the special relationship” between the United Kingdom’s Government Communications Headquarters (GCHQ) and the United States’ National Security Agency (NSA). The relationship between these two agencies has solidified over decades through close collaboration, primarily in the development of signals intelligence (SIGINT) technology, reporting, analysis, and language translation. Multiple veterans of these organizations remarked to the project researchers that, particularly before the post-9/11 intelligence integration reforms in the United States and the United Kingdom, they retained closer relationships with transatlantic colleagues than they did with other agencies in their own domestic intelligence communities.

Throughout World War II, the Cold War, the post-9/11 campaign against international terrorism, and now in the era of renewed global security competition, the SIGINT alliance has served as an unparalleled force multiplier for the United States, the United Kingdom, and the rest of the Five Eyes alliance. In some cases, participating services may focus on areas of prioritized strategic interest and share the outcomes of those operations with their international counterparts. In others, the baseline exchange of data across all five governments expands the quantity, quality, and diversity of insights, perspectives, and expertise for numerous missions.

More than 75 years of close collaboration has enabled GCHQ, NSA, and the other SIGINT elements of the Five Eyes alliance to codify a unique community and culture of shared knowledge, innovation, and capabilities. It is with an eye toward enabling the rest of the allied intelligence services to benefit from similar levels of collaboration that the authors propose this study’s intelligence reforms. There is certainly much room for the SIGINT agencies to benefit from these proposals. However, elements of the following recommendations may overlap with capabilities and efforts already present within the unique context of the SIGINT alliance. In these instances, NSA and GCHQ should play a leadership role in promoting the value of deep partnerships and serve as a model for the expansion of technical collaboration across the entire intelligence alliance. Although the SIGINT alliance cannot be replicated—and in some cases may not be effective for other aspects of the bilateral relationship—other U.S. and UK intelligence elements may have much to learn from this special relationship within the special relationship.

Promoting efforts to streamline collaboration between the United States and the United Kingdom does not mean that the two countries cannot pursue divergent interests. Indeed, some notable inconsistencies have recently emerged in the relationship, particularly as tensions between the United States and China continue to escalate at a pace not always matched by the United Kingdom and other U.S. allies in Europe. However, the bilateral relationship has long had flexibility for such differences, and the increasingly aggressive nature of actors like China, Russia, North Korea, and Iran is more likely to align transatlantic interests over time than push them apart. When it comes to intelligence, there will unquestionably be varying perspectives on threats and priorities, as well as sources, methods, and operations that cannot be shared.
This is understandable, and it is completely consistent with the recommendations that this report puts forward. This study ultimately advances a vision of broad-spectrum interoperability across the information sharing, security, acquisition, and technology domains of intelligence. The core motivation is to accelerate and maximize bilateral intelligence collaboration between the United States and the United Kingdom when both countries determine it is in their best interest to do so. Importantly, the individual lines of effort leave open the possibility of expansion, most immediately to other partners within the Five Eyes alliance. Just as the following technological, security, and policy recommendations are designed to enable robust collaboration, so too are the underpinnings of these ideas scalable and suitable for expansion to additional like-minded partners.

### PILLAR 1 MODERNIZE INFORMATION SHARING POLICY

**Finding:** Existing policies governing the release of intelligence information to foreign governments cannot meet the data challenges of the current technology environment.

**Recommendation 1:** The Office of the Director of National Intelligence (ODNI) should modernize U.S. intelligence community information sharing policies, particularly ICD 403.

#### MODERNIZE INFORMATION SHARING POLICY

<table>
<thead>
<tr>
<th>Finding</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing policies governing the release of intelligence information to foreign governments cannot meet the data challenges of the current technology environment.</td>
<td>The Office of the Director of National Intelligence (ODNI) should update U.S. intelligence community information sharing policies.</td>
</tr>
</tbody>
</table>

#### ENABLE JOINT TECHNOLOGY DEVELOPMENT

<table>
<thead>
<tr>
<th>Finding</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Despite repeated multilateral commitments to deepen cooperation on advanced and emerging technologies, significant roadblocks continue to impede efforts to build new joint capabilities.</td>
<td>The U.S. IC chief information officer (CIO) should partner with other U.S. intelligence component CIOs and their UK counterparts to develop an allied DevSecOps strategy.</td>
</tr>
</tbody>
</table>

#### PURSUE TRANSFORMATIONAL TECHNOLOGY

<table>
<thead>
<tr>
<th>Finding</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emerging technologies may offer opportunities to radically transform intelligence integration.</td>
<td>The United States, the United Kingdom, and Australia should develop a plan for achieving the AUKUS agreement’s vision of robust international collaboration on AI, quantum computing, and cyber capabilities.</td>
</tr>
</tbody>
</table>

**Source:** Authors’ own analysis.
program, are not designed to support information sharing at the scale and speed necessary to meet current and emerging challenges. The impact of classification and foreign disclosure policies on how the IC collaborates with partners can hardly be overstated. In January 2022, U.S. director of national intelligence (DNI) Avril Haines acknowledged that the current security classification system impedes the IC’s ability to share information with key partners.²⁵

The current U.S. policies on foreign intelligence disclosure—namely Intelligence Community Directive (ICD) 403 and Intelligence Community Policy Guidance (ICPG) 403.1—were issued in 2013.²⁶ These directives transitioned control of the IC’s foreign disclosure program to the ODNI from the director of the Central Intelligence Agency (CIA). While new roles and responsibilities were promulgated in ICD 403, the document in many ways carries forth the guidance from its predecessor, the 1998 Director of Central Intelligence Directive (DCID) 6/7.²⁷ As a result, information sharing policies still very much reflect a “tearline” approach.²⁸ Tearlines—which are created to release less sensitive portions of intelligence reports to a broader (and often international) audience—are an essential tool for sharing threat information. However, the labor-intensive process of creating tearlines cannot scale to the current and future information environment.

In both the United States and the United Kingdom, there are important legal and ethical reasons why certain intelligence requires additional scrutiny before disclosure. In the United States, this includes information collected under the Foreign Intelligence Surveillance Act (FISA), information about U.S. persons, and information that could be used by the recipient in support of lethal action.²⁹ In the United Kingdom, similar obligations under domestic and international law limit intelligence sharing with foreign partners, including the United States.³⁰ Nevertheless, in between the two extremes—on the one end, requiring foreign disclosure officers to approve each individual intelligence report for release and, on the other, the wholesale comingling of data—there are clear areas for improved collaboration.

A revised foreign disclosure policy should be evaluated with an eye toward tiered risk management. Current IC-wide policies are built to govern all instances of information sharing with no distinction between the Five Eyes intelligence partners and other nation-states.³¹ Given the close and enduring bonds across the Five Eyes alliance, the ODNI should introduce modernized guidance and protocols, under which information sharing with close allies and partners can be expedited. This may include expanding the corps of personnel at lower levels who, with appropriate training and documentation, may be authorized to share specified categories of information with certain partners. While individual agencies have undoubtedly found ways to enhance collaboration through their own agency-level implementations of ICD 403, the ODNI should establish formal and clear guidance that can streamline information sharing with close allies across the entire alliance.

**PILLAR 2**

**ENABLE JOINT TECHNOLOGY DEVELOPMENT**

Finding: Despite repeated multilateral commitments to deepen cooperation on emerging and advanced technologies, significant roadblocks continue to impede efforts to build new joint capabilities.

**Recommendation 2:** The U.S. IC chief information officer (CIO) should partner with other U.S. intelligence component CIOs and their UK counterparts to develop an allied DevSecOps strategy.

This recommendation is designed to build upon global software industry best practices in DevSecOps, particularly as they have been applied within the U.S. Air Force and increasingly across the broader U.S. Department of Defense (DoD) enterprise.³² The DoD Enterprise DevSecOps Strategy Guide, issued in March 2021, reflects many of the fundamental principles that should be adopted for an allied approach in intelligence.³³ In particular, the DoD has established several “software factories” that facilitate rapid development and deployment of new software capabilities by integrating a series of cultural, technical, and security approaches.³⁴ The establishment of similar U.S.-UK software factories would enable rapid prototyping and development of tools for, among many things, conducting data analytics and accelerating information sharing between intelligence teams. Such components could also be designed to accommodate for differences in broader government technology strategies, particularly in cloud computing. That is, regardless of either government’s cloud computing strategy—both of which have been embroiled in recent controversy—joint DevSecOps strategy should be designed according to a “build once, run anywhere” approach.³⁵ This will allow for deployment of software on commercial cloud, in on-premise data centers, or even embedded in collection sensors or weapons platforms.
Shifting from the legacy “waterfall” development model to a DevSecOps approach represents a move away from static, requirements-driven software development to an iterative model that emphasizes rapid delivery and continuous improvement. It is a necessary evolution for any intelligence agency that aspires to be truly innovative in the digital age. Moreover, the “security” in DevSecOps includes the integration of a wide range of best practices in secure software development that facilitate real-time awareness of the software’s integrity and reliability. Over time, a common reference framework guiding the development of joint capabilities could evolve into a common standard, not only for U.S. and UK technology development and capability exchange, but for the broader Five Eyes intelligence alliance as well.

**Recommendation 3:** The U.S. Department of State, in coordination with the Department of Defense, the Department of Commerce, and the U.S. IC, should work with their British and Australian counterparts to develop a clear plan for achieving the AUKUS agreement’s vision of robust international collaboration on AI, quantum computing, and cyber capabilities.

The 2021 AUKUS agreement reflects a key milestone in the reaffirmation of the importance of the partnership between the United States, the United Kingdom, and Australia. Although much of the immediate attention directed toward AUKUS has been on the agreed delivery of nuclear-powered submarines to Australia, the agreement also commits the three nations to “foster deeper integration of security and defense-related science, technology, industrial bases, and supply chains,” specifically in the areas of cyber capabilities, AI, and quantum computing. While the commitment to deeper collaboration on these emerging and advanced technologies is commendable, this study repeatedly encountered a series of policy, regulatory, and cultural challenges that will greatly inhibit such efforts.

Notable obstacles in this area include the U.S. International Traffic in Arms Regulations (ITAR) and the U.S. Export Administration Regulations (EAR), as well as these regimes’ counterparts in the United Kingdom. Despite multiple efforts over the years to integrate the industrial bases of close allies and partners, such initiatives have largely failed to meet the challenges of the current technology landscape. For example, the National Technology and Industrial Base (NTIB), which was designed to streamline technology collaboration between the United States, Australia, Canada, and the United Kingdom, has failed to deliver on its vision, according to multiple in-depth studies.

Reconciling the friction between existing technology transfer practices and the grand ambitions of AUKUS may prove to be one of the agreement’s greatest challenges. For its part, the U.S. Congress has recognized the importance of joint technology development as an element of broader technology competition. As of early 2022, both chambers had passed legislation directing the U.S. secretary of state to conduct an NTIB study, which would evaluate the barriers to achieving the goals of the initiative both within the United States and in partner nations.

**Reconciling the friction between existing technology transfer practices and the grand ambitions of AUKUS may prove to be one of the agreement’s greatest challenges.**

Although technology transfer issues are commonly associated with defense cooperation, they are increasingly relevant to the intelligence mission. As reflected in the AUKUS agreement, the suite of technologies at the core of strategic competition with China—AI, cyber capabilities, and quantum computing—are crucial to the future success of intelligence agencies. The United States, the United Kingdom, and Australia should seize AUKUS as an opportunity to achieve the level of joint technology development that all three countries have repeatedly committed to.

**Recommendation 4:** The U.S. National Counterintelligence and Security Center—in coordination with IC information and acquisition security officials, the Department of Defense, the Department of State, and the Department of Commerce—should explore how acquisition security and foreign ownership, control, and influence (FOCI) policies could more effectively balance risk between close allies and threat actors.

As reflected in U.S. and UK strategies, partnering with commercial entities to develop emerging technologies is an essential national security imperative. At the same time, technology research, development, and production are increasingly international. Today, collaboration between universities, corporations, and venture capitalists outside of the national security space is borderless. Despite this reality, government risk management of technology in many ways mirrors the challenges this study identified in existing U.S. information sharing policies. That is, policies...
governing firms and individuals with foreign ties largely adhere to standards that do not differentiate between allies and adversaries.

The high level of economic interdependence between the United States and the United Kingdom necessitates reevaluation of how technology with ties to either country is vetted for counterintelligence and security risks by the other. By one estimate, between 1976 and 2015, the United Kingdom was the fourth-largest foreign investor in U.S.-based technology startups.\(^{43}\) British investment in the United States in 2019 accounted for more than 25.3 percent of the United Kingdom’s outward investment.\(^{44}\) Conversely, U.S. investment accounted for more than 25 percent of all UK inward foreign direct investment (FDI).\(^{45}\)

Despite this level of economic partnership between close allies, several individuals consulted in support of this project—both American and British—stated that they knew of specific cases where the application of existing acquisition security or FOCI policies limited government innovation. These issues can arise for many reasons. For example, startups looking to contract with the U.S. government that receive venture capital from foreign sources are all subject to the same interminable acquisition security reviews, regardless of whether their funding originates from a close ally or a threat actor. For many small, highly innovative firms from allied nations, this process is financially unsustainable and serves as a deterrent from attempting to partner with the U.S. government.

Overlaying these acquisition security and FOCI challenges is the reality that the software industry is truly global. The diverse and often highly specialized expertise retained by software developers around the globe is a necessary input for innovation, particularly in the areas of emerging and disruptive technologies. The underlying software driving the global revolutions in machine learning and DevSecOps is, in many cases, free and open-source software (FOSS) managed by programmers scattered throughout the world. Intelligence services seeking to innovate should not resist these models, despite the fact that they undoubtedly carry risk. The late 2021 discovery of a vulnerability in Log4j, an open-source library deployed in billions of devices globally, is merely the latest high-profile incident underscoring the complexities and dangers inherent in modern software development.\(^{46}\) Nevertheless, as MI6 chief Richard Moore recently acknowledged in public remarks, “We [cannot] match the scale and resources of the global tech industry, so we shouldn’t try. Instead, we should seek their help.”\(^{47}\)

**The high level of economic interdependence between the United States and the United Kingdom necessitates reevaluation of how technology with ties to either country is vetted for counterintelligence and security risks by the other.**

At the heart of a continued pivot to deeper collaboration with private industry should be efforts to adopt zero trust best practices. As reflected in ongoing U.S. and UK efforts to embrace zero trust architecture and promote secure software development, the transparency inherent in these approaches increases opportunities to collaborate with diverse partners.\(^{48}\) Software bills of materials (SBOMs), continuous security auditing (implemented according to a DevSecOps playbook), and other secure software supply chain best practices are designed to minimize risk, no matter who designed the software.

Ideally, a zero trust approach would allow intelligence agencies to benefit from more bleeding edge capabilities. Existing FOCI processes often prohibit foreign nationals or uncleared citizens from working on a project. Such strict personnel security measures may be necessary when systems and capabilities are highly sensitive, but these practices have a cost. In the software world, it means that the pool of talent capable of working on a project rapidly declines, potentially restricting access to necessary expertise and likely resulting in inferior or outdated capabilities.

An acquisition model that requires software to be built according to zero trust principles can potentially mitigate traditional FOCI and other personnel security concerns. If the transparency and integrity of software can be verified continuously, intelligence agencies may, in some circumstances, be able to purchase and deploy software that may have not been approved under legacy FOCI processes. By developing processes to verify trust in software—regardless of its origin—the potential pathways to rapid innovation will expand tremendously.

**PILLAR 3**

**PURSUE TRANSFORMATIONAL TECHNOLOGY**

**Finding:** Emerging technologies may offer opportunities to radically transform international intelligence collaboration.
Recommendation 5: The U.S. Intelligence Advanced Research Projects Agency (IARPA), partnering with appropriate UK partners, should spearhead efforts to evaluate how privacy enhancing technologies (PETs) could enhance bilateral data analytics in compliance with existing information sharing regulations.

Throughout this study, the research team repeatedly explored the concept of a bilateral “data lake” wherein operational data and analysis—as agreed to under broad bilateral sharing agreements—could be pushed automatically to users in the United States and the United Kingdom as it was generated. Despite reflecting the ultimate vision of interoperability, such a model cannot be reconciled with existing domestic and international legal and regulatory obligations.

If information sharing continues to be conducted according to legacy models, which largely rely on transmitting and replicating data within the geographical and network boundaries of the partner nation, existing restrictions governing sharing have little room for modernization. Although Pillar 2 proposes a vision for developing joint technology for exchanging knowledge, tools, and data, those capabilities will be bound to predefined parameters consistent with their design and operational purpose.

A host of emerging technologies, however, carry the potential to introduce new models to facilitate bilateral data analytics without necessarily granting unrestricted access to the underlying information. Various PETs are currently being developed and evaluated for use in fields where broad insight into protected data delivers important benefits but the information itself is too sensitive for full, unencrypted access. Tools such as homomorphic encryption, differential privacy, zero knowledge proofs, and other “structured transparency” approaches have proven widespread applications in fields like healthcare, but intelligence agencies would greatly benefit from similar capabilities.49

One of the most important benefits of a theoretical U.S.-UK data lake would be the ability for both nations to expand their access to the essential “data fuel” upon which machine learning (ML) and AI capabilities rely. PETs can supplement these capabilities by enabling the performance of trusted analytics over bulk data without granting access to specific, sensitive information within the dataset itself. This can allow AI/ML systems to generate better data-informed insights without deanonymizing the specific details of any individual data entry. Both crafting the appropriate technical infrastructure to facilitate the joint use of such technologies and developing effective oversight mechanisms to govern the use of such capabilities will require extensive effort. Nonetheless, the benefits of such approaches could be significant, not only in paving the way for more robust joint data analytics but also for each individual nation’s efforts to ensure that its use of emerging and advanced technologies for intelligence purposes aligns with fundamental respect for privacy, transparency, and human rights.

The research team is highly encouraged by recent bilateral work in this area, specifically the announcement in December 2021 that the United States and the United Kingdom are jointly sponsoring a series of innovation prize challenges focused on advancing PETs as a core pillar of efforts to advocate a suite of “democracy-affirming technologies.”50 This emphasis on PETs complements broader efforts to, in the words of the former U.S. director of the Office of Science and Technology Policy, Dr. Eric Lander, “support our shared democratic values in the face of authoritarian exploitation of emerging technologies.”51

Recommendation 6: The U.S. IC CIO should work with U.S. IC components and their UK counterparts to evaluate how AI can automate existing information sharing processes.

As discussed in Pillar 1, current information sharing policies must be modernized, particularly those governing the U.S. IC’s foreign disclosure program. Concurrent with efforts to streamline the IC’s ability to share intelligence information with close allies, the United States and the United Kingdom should investigate how tearline processes can be automated using AI capabilities. For example, ongoing work in the field of natural language processing (NLP) may have useful applications for rapidly generating summaries of longer texts. When creating tearlines, intelligence officers typically need to review a full intelligence report, identify the key elements of information from that report, and write a synopsis that captures that information in a way that protects sensitive sources and methods. It is possible to envision how NLP-enabled AI, partnered with human evaluators, could be trained over time to generate high quality tearlines at far greater speeds than humans doing the task alone. In the current threat environment, decision cycles are short, and the rapid release of information to a broad range of partners—foreign intelligence services, the private sector, nongovernment entities, and the public—is essential.
In addition to speeding up processes, AI tools carry the potential to reduce the administrative and workforce burdens associated with current models of information sharing, allowing resources and personnel to be allocated to other missions.

CONCLUSION

One question that this report has not answered is whether the special relationship is still, to put it simply, special. Accounts of its decline (or rebirth) can be traced back decades. Such reappraisals of the utility and purpose of alliances are entirely healthy, particularly when these efforts breathe new life into long-standing partnerships. This report, however, is not intended to forecast the trajectory of the relationship. Rather, it attempts to point stakeholders toward options to enhance U.S.-UK intelligence interoperability. In so doing, it assumes that the enduring value of the relationship is twofold.

First, there remains tremendous value in what U.S.-UK cooperation means. As described from the outset of this report, a core component of strategic competition in this era will be about building alliances of like-minded nations to push back against authoritarianism that runs contrary to core democratic values. At the highest levels, intelligence leaders of both countries have started to recognize that articulating shared threats and demonstrating common ideals are crucial steps in the emerging confrontation over ideas. The second reason the U.S.-UK relationship remains special is because of what it does. For good reason, the alliance is celebrated for its successes over the past 75 years. Despite these decades of deep integration and cooperation, however, there exists today a significant misalignment between the strategic prioritization of the U.S.-UK alliance—reflected in AUKUS, the new Atlantic Charter, and domestic national security strategies in both Washington and London—and the regulations, policies, organizational cultures, and technologies that facilitate its day-to-day activities. Without the necessary improvements, it is only a matter of time before renewed ambitions for even stronger defense and intelligence partnerships, built to prevail in a long-term competition with rising powers, will collide with the reality of often inflexible, risk-averse, and outdated policies, processes, and tools. In this regard, reforming old policies, adopting new models, and building novel capabilities to deepen and streamline collaboration will be critical to the future of intelligence missions. After all, to remain secret, U.S. and UK intelligence services must become more open to one another.

Jake Harrington is an intelligence fellow with the International Security Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C. Riley McCabe is a research assistant with the CSIS International Security Program.

This brief is made possible by support from Rebellion Defense.

The Royal United Services Institute (RUSI) is the United Kingdom’s leading independent, not-for-profit research institute for security studies. RUSI specializes in facilitating contact between academics, policymakers, and practitioners in security fields to bring together research, policy, and practice. Its mission is to inform, influence, and enhance public debate on a safer and more stable world. This research paper builds on RUSI’s considerable work in the field of intelligence and security policy in recent years, which has provided an independent, objective analysis of key policy issues, drawing on multidisciplinary expertise from leading academics and practitioners.

RUSI’s role in this project was to assist the CSIS team in shaping research questions and the strategic direction of the research, provide support in setting up a research-based workshop, participate in interviews with UK-based stakeholders, input peer review and advice from a UK perspective, and disseminate the paper’s findings across RUSI’s network in the security and defense space.
ENDNOTES


21 Nakasone and Fleming, “75UKUSA.”

22 For additional background on the strength and legacy of the GCHQ-NSA relationship, see Robert Joyce’s remarks at the Intelligence and National Security Alliance on January 15, 2021, https://
Rajeev Syal, “Priti Patel pressed to explain award of spy agencies


The U.S. intelligence community defines tearlines as “portions of an intelligence report or product that provide the substance of a more highly classified or controlled report without identifying sensitive sources, methods, or other operational information. Tearlines release classified information with less restrictive dissemination controls, and, when possible, at a lower classification.” For additional background on tearlines, see Intelligence Community Directive (ICD) 209, available at https://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf.


“Intelligence Directive 403,” ODNI.


For additional background on Department of Defense software factories, see “Software Factories,” Office of the Chief Software Officer, https://software.army.mil/software-factories/.


Department of Defense, DoD Enterprise DevSecOps Strategy Guide.


Ibid.


Ibid.


Moore, “Human Intelligence in the Digital Age.”


Ibid.