United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits

May 15, 2019

Congressional Research Service
https://crsreports.congress.gov
R45720

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R45720

May 15, 2019

Michael E. DeVine
Analyst in Intelligence and National Security

United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits

From its inception, the United States Intelligence Community (IC) has relied on close relations with foreign partners. These relationships often reflect mutual security interests and the trust each side has of the other's credibility and professionalism. They are generally strategic and cover a range of national security priorities involving national defense, emerging threats, counterterrorism, counter-proliferation, treaty compliance, cybersecurity, economic and financial security, counter-narcotics, and piracy.

U.S. intelligence relations with foreign counterparts offer a number of benefits: indications and warning of an attack, expanded geographic coverage, corroboration of national sources, accelerated access to a contingency area, and a diplomatic backchannel. They also present risks of compromise due to poor security, espionage, geopolitical turmoil, manipulation to influence policy, incomplete vetting of foreign sources, over-reliance on a foreign partner's intelligence capabilities, and concern over a partner's potentially illegal or unethical tradecraft. Because intelligence failures involving a foreign partner sometimes become public, the risks to the IC of cooperating with a foreign intelligence service are more easily understood. Nevertheless, the persistent cultivation of intelligence relations with foreign partners suggests that the IC remains confident that the benefits outweigh the risks.

These benefits are not always widely recognized due to their sensitivity and the potential for compromising the scope and details of what amounts to intelligence collection. The best known of these intelligence relationships are the decades-long ties to America's closest allies, who have shared history, values, and similar perspectives on national security threats. Such ties are often one component of a broader security cooperation arrangement. Less well known are liaison relationships with U.S. adversaries over a particular issue of mutual concern, or relations with non-state foreign intelligence organizations such as Kurdish groups. Regardless of the partner, the U.S. Intelligence Community's aim is to enhance national intelligence resources and capabilities and to further U.S. national security by better understanding the threat environment and thereby enabling informed strategic planning, better policy decisions, and successful military operations. Thus, U.S. foreign intelligence relationships can be an overlooked component of public discussion of various aspects of international cooperation.

Foreign intelligence agencies with ties to U.S. intelligence have often escaped the reach of congressional oversight. Yet Congress, at various times, has been interested in both the benefits and the risks of foreign intelligence relationships to U.S. national security. While sometimes extolling the value intelligence foreign partners can provide, Congress has also been critical of occasions when the IC has become too dependent on such partners at the expense of IC investment in its own intelligence capabilities. Congress has also been concerned with the IC's ability to independently assess the credibility of foreign intelligence sources, as well as the vulnerability of a foreign intelligence partner's telecommunications infrastructure to compromise by a hostile foreign intelligence service. Of particular sensitivity to Congress has been the poor record of human rights by certain foreign intelligence agencies and the potential for foreign intelligence partners to collect and share with the United States information on U.S. persons.

This report uses publicly available, unclassified sources as the basis of its research, and does not reference information in the public domain that was unlawfully disclosed.

Contents

Contacts

Introduction

U.S. foreign intelligence relations are a component of U.S. international relations that involve cooperation between a U.S. and a foreign state or non-state intelligence service over an area of mutual interest. This cooperation may include simple liaison to discuss or exchange information, raw data, or finished intelligence. Intelligence liaison leverages the relative strengths of the interested intelligence services to provide tactical, operational, or strategic insight and perspective to provide warning of attack, corroboration of national sources, or additional, possibly unique, intelligence that the other service lacks. Other forms of cooperation include basing rights to enhance the range of U.S. collection coverage, joint operations and collection from the sovereign territory of a foreign state, and training to improve the capacity and professionalism of a foreign intelligence service. In areas of the world where the U.S. Intelligence Community (IC) has few national intelligence assets, cooperative relations with a foreign intelligence service based in the region can effectively increase the range of U.S. intelligence coverage by using the partner's source network and linguistic, political, and cultural expertise. Although the Director of National Intelligence (DNI) provides the policy and criteria, and conducts oversight for all IC element intelligence relationships with foreign intelligence services, the IC elements themselves have the statutory authority to enter into agreements with foreign counterparts.[1] Normally every relationship is formalized through a memorandum of understanding (MOU) or other written agreement.

This report provides a historic perspective of traditional and nontraditional foreign intelligence partnerships with the U.S. It also discusses their risks and benefits in the context of the broader public discussion over the sorts of relationships the United States should have with various actors in the international community. In many—but not all—instances, intelligence relations with a foreign partner may be viewed as an approximate reflection of the strategic condition of the relationship between the U.S. and that partner generally. They indicate shared interests and a degree of trust in the professional ability of the partner to provide credible intelligence while protecting sources and maintaining security about the nature and extent of the relationship. In discussing risk, this report emphasizes the risk to the United States. However, foreign partners also bear risk (e.g., relying too heavily on U.S. intelligence, or having their sensitive sources compromised).

Congress has a vested interest in understanding the nature and scope of the IC's relations with foreign intelligence services. Congress has expressed both confidence in the value of these relationships and reservations. When the IC reduced national intelligence collection resources in the 1970s and the 1990s and the IC became heavily dependent upon intelligence obtained from foreign partners,[2] Congress intervened to rebalance national intelligence collection with collection from foreign partners.[3] Congress was also critical of deficiencies in the IC's ability to

[1] 50 *U.S.C.* §3001, E.O. 12333, *United States Intelligence Activities.*

[2] The reductions in the 1970s and 1990s were precipitated, respectively, by the discovery of CIA abuses of its authority in conducting domestic surveillance of anti-Vietnam war activities, and the end of the Cold War, with the IC's de-emphasis of collection on the former Soviet Union. On those occasions, over-reliance on reporting from particular foreign intelligence services, as a way of compensating for the reduction in United States collection, resulted in the IC being surprised by the level of unrest in Iran prior to the fall of the Shah in 1979, and in the IC's relative lack of access to Al Qa'ida prior to the 9/11 attacks, as described later in this report.

[3] See, for example, U.S. Congress, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* (Washington, DC: U.S. Government Printing Office, December 2002), p. 91, at

assess independently the credibility of foreign intelligence sources, one of whom fabricated reporting on Iraqi weapons of mass destruction, one reason cited by the Bush Administration for invading Iraq in 2003.[4] Most recently, Congress has expressed interest in the vulnerability of foreign intelligence partners' telecommunications technology to penetration by hostile intelligence services.[5]

Note on Sources

Much of what could be known of U.S. intelligence relations with foreign partners is sensitive, remains classified, and, therefore, cannot be included in this report. However, this report can serve as a general reference to enable an informed perspective on the benefits as well as the risks of foreign intelligence relationships to U.S. national security. It uses publicly available, unclassified sources as the basis of its research, and does not reference information in the public domain that was unlawfully disclosed. Examples cited are also historical and do not necessarily provide a general characterization of the current relationship between the United States and a particular foreign partner.

Background and Historical Context

The United States has cultivated intelligence liaison relations with foreign partners through (1) the exchange of information, raw data, or finished intelligence;[6] (2) basing rights for conducting intelligence operations, or privileges to host technical intelligence equipment; (3) burden sharing in the collection and reporting on issues of mutual interest; (4) joint covert action, collection, or exploitation operations; and (5) training. Most are bilateral. The relationship with the United Kingdom is among the oldest and the best known. The IC also has multilateral relationships, with NATO member states, Five Eyes partners (United States, United Kingdom, Canada, Australia, and New Zealand), and the intelligence organizations supporting coalition partners in operational theaters such as Iraq and Afghanistan.[7]

U.S. IC relationships with foreign intelligence partners have developed in parallel with global IC coverage, as well as the growing number of interests the U.S. shares with foreign partners; it is also generally recognized that intelligence partnerships can provide mutual benefits for national security. IC foreign partnerships have developed as consequences of the most pressing challenges for U.S. national security over the past century: two world wars, the Cold War, and post-9/11 counter-terrorism operations. Although the U.S. has periodically shared intelligence with adversaries involving a narrow range of mutual interests, this type of exchange represents the exception to the norm. More typically, most intelligence sharing takes place with allied countries or U.S. affiliated non-state actors within relationships that have been shaped by decades of shared experience in war and peace. U.S. intelligence exchange relationships with foreign partners, therefore, often reflect the high level of trust and professional confidence the U.S. IC places in

https://www.intelligence.senate.gov/sites/default/files/documents/CRPT-107srpt351-5.pdf.

[4] Rafid Ahmed Alwan al-Janabi, code-named "Curveball," was the source of the German Federal Intelligence Service (Bundesnachrichtendienst, or BND) who fabricated reporting that Saddam Hussein's Iraq possessed weapons of mass destruction.

[5] See, for example, S. 245, Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019 (116th Congress), Section 307.

[6] Intelligence is information that has been evaluated for national security significance. Raw data is data that has not been analyzed. Finished intelligence is intelligence—information that has been evaluated for national security significance—resulting from the integration of multiple intelligence sources.

[7] There is, however, a statutory prohibition from sharing intelligence with the United Nations unless the President waives this provision in the interests of U.S. national security. See 50 U.S.C. §3047(a)(1)-(2).

partnerships with particular foreign allies' intelligence services, involving a broad range of overlapping national security, political, and economic interests.[8] A fundamental assumption, supported by decades of experience, is that building and maintaining these partnerships enhances U.S. national security by providing some benefit that the U.S. would otherwise lack: access to otherwise inaccessible or hostile targets, corroboration of sources, cultural or linguistic expertise, the capacity to conduct joint assessments, providing indications and warning of an attack, obtaining basing rights, or jointly planning and conducting covert operations or intelligence collection.

Early Years

The earliest efforts by the United States to formally cooperate with foreign partners in intelligence took place during World War I, when the British and French provided training, advice, and tactical intelligence exchanges with the American Expeditionary Force (AEF) under General John Pershing.[9] At the time, the United States had only an incipient intelligence capability. The British, in contrast, had had a national intelligence service since 1909 when the Secret Service Bureau was established to address growing concerns about a perceived threat posed by imperial Germany.[10]

The United States forged closer intelligence ties with allied governments in the years leading up to World War II and during the war itself. The UK and U.S. navies began sharing naval intelligence in the 1930s. The first formal arrangement, involving signals intelligence, was reached in October 1942 when the U.S. Navy and British Government Code and Cypher School (GC & CS) at Bletchley Park signed the Holden Agreement. That agreement enabled collaboration on Japanese, German, and Italian signals intelligence targets that included a division of labor between each side for more streamlined, integrated technical collection and analysis.[11] The British-U.S. communication intelligence agreement (BRUSA Agreement) signed in 1943 between GC & CS and the U.S. War Department—representing the Army as well as the Navy signals intelligence capabilities—superseded the Holden Agreement. This agreement also provided for a division of labor similar to the Holden Agreement, whereby the United States had responsibility for collection of signals intelligence targeting the Japanese (an operation called Magic), and the British had responsibility for collection of signals intelligence on German and Italian targets (referred to as Ultra).[12] This collaboration proved pivotal in the Allies establishing information dominance during the war.

---

[8] A former Director of the CIA, for example, characterized the intelligence relationship between the United States and the United Kingdom as "ties [that] are and always will be essential to our collective security." "John Brennan on Transnational Threats to Global Security," *Council on Foreign Relations,* June 29, 2016, at https://www.cfr.org/event/john-brennan-transnational-threats-global-security.

[9] Michael Warner, *The Rise and Fall of Intelligence: An International Security History* (Washington, DC: Georgetown University Press, 2014), pp. 60-63.

[10] The Secret Intelligence Bureau was organized into domestic and foreign sections which today are represented by two separate organizations: the Security Service (MI5) and the Secret Intelligence Service (SIS/MI6), respectively. See "Our History," Secret Intelligence Service/MI6, at https://www.sis.gov.uk/our-history.html.

[11] See Ralph Erskine, "The Holden Agreement on Naval Sigint: The First BRUSA?" *Journal of Intelligence and National Security*, Vol. 14, Issue 2, (1999), pp. 187-197, at https://doi.org/10.1080/02684529908432545.

[12] See "An Agreement between British Government Code and Cipher School and U.S. War Department in Regard to Certain 'Special Intelligence,'" National Security Agency, at https://www.nsa.gov/news-features/declassified-documents/ukusa/. The agreement's accompanying War Department cover memorandum is dated June 10, 1943. The agreement itself is dated May 17, 1943.

Cold War

Shared interests during the Cold War influenced the next period in the evolution of U.S. foreign intelligence partnerships. U.S. intelligence relations with traditional allies solidified as one of multiple areas of security cooperation based on a shared perception of the threat posed by the Soviet Union. The UKUSA Agreement of March 1946 superseded the BRUSA Agreement and other U.S.-UK signals intelligence agreements from WWII that had focused exclusively on targeting the Axis powers.[13] The UKUSA Agreement added the State Department, the Army, and Navy on the U.S. side of the board overseeing the partnership. The agreement provided for an expanded exchange of signals intelligence-related products and services concerning targets involving "any country … excluding only the U.S., the British Commonwealth of Nations, and the British Empire."[14] Canada, Australia, and New Zealand were formally included as "collaborating" partners in the late 1940s and early 1950s. Subsequently, in a separate agreement, the United States and United Kingdom formally established standards for the protection of classified information involved in exchanges.[15]

Before the establishment of the Office of Strategic Services (OSS) in 1942 with the encouragement and assistance of the United Kingdom, the United States had no foreign intelligence collection or covert action capability to compare to the capabilities of Britain's Secret Intelligence Service (MI6).[16] The WWII experience of OSS personnel and the investment the United States made in national intelligence (including establishing the CIA in 1947),[17] enabled the U.S. to influence the organization and development of other nations' intelligence agencies; these agencies have since become close bilateral partners.

One example is the establishment of the West German Federal Intelligence Service, the Bundesnachrichtendienst (BND). In 1946 the former head of the eastern branch of the Nazi German intelligence, Reinhard Gehlen, who was responsible for intelligence targeting the Soviet Union, negotiated terms for establishing an intelligence organization in occupied postwar Germany with the United States.[18] During the war, Gehlen had developed extensive agent networks, and had later copied and concealed for safekeeping voluminous amounts of intelligence

[13] For a complete reference of declassified signals intelligence agreements and related documents between the United States and United Kingdom from 1943-1961, see the National Security Agency's site at https://www.nsa.gov/news-features/declassified-documents/ukusa/.

[14] *British-U.S. Communication Intelligence Agreement*, March 5, 1946, declassified and approved for release by NSA, at https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/ukusa/agreement_outline_5mar46.pdf.

[15] *General Security Agreement*, April 14, 1961, declassified and approved for release by the Department of State, at https://www.documentcloud.org/documents/4443925-2017-11-02-Privacy-International-State-Production.html. Bilateral intelligence exchange agreements often have a third-party rule that prohibits the dissemination of intelligence to a third party, to include another foreign intelligence entity or even oversight organization, without the authorization of the intelligence organization that originated the intelligence in question. See also Scarlet Kim, Diana Lee, Asaf Lubin, and Paulina Perlin, "Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements," *Lawfare*, April 23, 2018, at https://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing.

[16] For an account of the British influence on the establishment of the OSS, see Joseph F. Jakub III, *Spies and Saboteurs: Anglo-American Collaboration and Rivalry in Human Intelligence Collection and Special Operations, 1940-45* (London: Palgrave Macmillan, 1999), pp. 23-28.

[17] The CIA was established by §102 of the National Security Act of 1947 (P.L. 253-80), codified as 50 *U.S.C.* §3035(a)-(b).

[18] Gehlen commanded Foreign Armies East, one of two branches of the Abwehr, the Nazi German intelligence organization responsible for intelligence on foreign militaries.

on the Soviet Union that he knew would be valuable to the United States. Using this leverage, Gehlen, following his surrender, was able to obtain U.S. support for an autonomous German intelligence organization for collecting and analyzing intelligence on the Soviet Union and other communist states that would become part of a reconstituted German government. The Gehlen Organization, as it was known, became the BND in 1956 and has remained a close, albeit independent, partner of the United States IC.[19]

Similarly, the United States was influential in the early years of the Mossad, Israel's human intelligence agency. The Mossad, like the Gehlen organization, provided the United States a means to acquire information on the Soviet Union that the United States could not otherwise collect through national sources, as Israel was able to draw upon its eastern European émigré population's extensive contacts in the Soviet Union. The CIA, in turn, was able to offer training to Mossad agents.[20]

U.S. relations with the intelligence organizations of Japan, Egypt, pre-revolutionary Iran, Saudi Arabia, and Pakistan were also influenced by mutual concern over the threat from the Soviet Union. The Soviet invasion of Afghanistan in 1979, in particular, contributed to the CIA's forming closer ties to Saudi Arabia's General Intelligence Directorate (GID) and Pakistan's Inter-Services Intelligence (ISI) agency in an effort to provide funding and other covert assistance to the Mujahideen.[21]

Post-Cold War

After the Cold War, former communist countries that had long been allied with the Soviet Union became NATO allies and intelligence partners of the United States (i.e., Poland, Hungary, Czechoslovakia (now the Czech Republic and Slovakia), Bulgaria, Romania, and the Baltic states of Estonia, Latvia, and Lithuania). Initially, there was some ambivalence about these new partnerships. On one hand, the history of Soviet influence over Warsaw Pact intelligence organizations suggested the reconstituted intelligence agencies of the eastern European NATO states could pose a counterintelligence risk of Russian penetration and result in greater restraint in intelligence sharing. On the other hand, by virtue of these services' extensive experience with the Soviets Union, they might prove more capable of providing for themselves protections against Russian penetration.[22] These services offered not only a presumable wealth of perspective on and access to post-communist Russia, but also support for the U.S. in other areas of the world where they had had operational experience, extensive contacts, or were commitment to supporting NATO or U.S.-led military coalition operations. In some cases (e.g., the Polish presence in Iraq),

[19] See Jeffrey T. Richelson, *Foreign Intelligence Organizations* (Cambridge: Ballinger Publishing Co., 1988), pp. 132-136. See also Jens Wegner, "Shaping Germany's Post-War Intelligence Service: The Gehlen Organization, the U.S. Army, and Central Intelligence, 1945-1949," *Journal of Intelligence History*, vol. 7 (Summer 2007).

[20] See Ephraim Kahana, "Mossad-CIA Cooperation," *International Journal of Intelligence and Counterintelligence*, vol. 14, no. 3 (2001), at https://www.tandfonline.com/doi/pdf/10.1080/08850600152386873?needAccess=true.

[21] See, for example, Bruce Riedel, *What We Won: America's Secret War in Afghanistan, 1979-89* (Washington, DC: The Brookings Institution, 2014). The CIA's relations with ISI have subsequently been challenged by ISI's perceived support for proxy Islamist groups.

[22] Following the 1989 overthrow of the communist government, out of 1,000 agents in the Polish intelligence Office of State Security, the government reportedly purged 600 who were seen as sympathetic to Russia. The Czech Republic went further, establishing an entirely new domestic and foreign intelligence services to replace the State Security Service (StB) that existed under the communist regime. At the same time, there was relatively little turnover of personnel in Hungarian intelligence, however. See Jane Perlez, "Touchy Issue of Bigger NATO: Spy Agencies," *The New York Times*, January 5, 1998, at https://www.nytimes.com/1998/01/05/world/touchy-issue-of-bigger-nato-spy-agencies.html.

part of the motivation may have been simply to gain western or NATO experience and prove their worth as a reliable ally and intelligence partner.[23]

In the aftermath of the terrorist attacks of 9/11, the U.S. IC expanded its foreign intelligence liaison relationships as a major component of counterterrorist strategy. Working with intelligence partners in the war on terror is broadly viewed as essential to protecting the U.S. homeland and the allied states who share western values that make them attractive targets for al Qa'ida, and the so-called Islamic State.[24] These relationships include nontraditional partners, in addition to allies: non-state organizations (such as Kurdish groups in northern Iraq and Syria) and traditional adversaries such as Russia. The CIA has solidified many of these partnerships through the establishment of a network of Counterterrorist Intelligence Centers (CTIC) around the world to facilitate sharing intelligence on terrorism, such as indications and warning of an attack, with a host-nation government to effect the killing or capture of high-value targets. The Counterterrorist Center (CTC) at CIA headquarters manages the CTICs overseas. The National Security Agency (NSA) is also represented in the CTICs, underscoring the importance of signals intelligence (and the corresponding foreign partnerships) to counterterrorist operations.[25] Simultaneously, the U.S. IC has found that nontraditional partners remain loyal to their own interests and internal dynamics despite heavy inducement by the U.S.[26] While these partnerships have proven valuable in certain circumstances, they are not all completely beneficial to the U.S.

Each period in the evolution of U.S. intelligence relations with foreign partners—Pre-World War II, World War II, the Cold War, Post-Cold war —has enabled the United States to strengthen ties to traditional allies, while presenting challenges from necessary yet incompletely reliable partners. The post-Cold War has been marked by a concerted effort to forge or strengthen ties with allies old and new, and to expand the scope of counterterrorism coverage by initiating or increasing the frequency of intelligence exchanges with nontraditional intelligence partners.

Policy and Legal Authorities

Policy and authorities for initiating and managing ties between the IC and foreign intelligence services, and specifying the roles and responsibilities of personnel supporting these relationships, are found in statute, executive orders, and intelligence directives.

[23] Ibid. Polish intelligence helped extricate CIA personnel from Iraq in 1990 prior to the Gulf War. Polish intelligence personnel also supported the U.S.-led Multi-National Forces in Iraq (MNFI) coalition subsequent to the 2003 invasion, as well as the NATO mission in Afghanistan.

[24] Dana Priest, "Foreign Network at Front of CIA's Terror Fight," *Washington Post*, November 18, 2005, athttp://www.washingtonpost.com/wp-dyn/content/article/2005/11/17/AR2005111702070.html.

[25] Ibid. The CTICs were first reported in this *Washington Post* article by Dana Priest. Indonesia, Uzbekistan and France were reported as some of the countries where CTICs were located. The CTIC in Paris, France, called *Alliance Base*, in operation from 2002-2009, and involved not only the U.S. and France as partners, but also Britain, Germany, Canada and Australia. Then French President Jacques Chirac directed French intelligence services, the DGSE and DGSI, share intelligence with the U.S. "as if they were your own service." See Dana Priest, "Help from France Key in Covert Operations," *Washington Post*, July 3, 2005, at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/02/AR2005070201361.html.

[26] See for example https://www.newyorker.com/news/news-desk/the-cias-maddening-relationship-with-pakistan; https://www.theatlantic.com/international/archive/2018/10/jamal-khashoggi-american-saudi-counterterrorism-relationship/573148/

Intelligence Community Directive (ICD)-403, *Foreign Disclosure and Release of Classified National Intelligence,* states U.S. Government policy on disclosure of U.S. intelligence to foreign state or non-state intelligence entities:[27]

> U.S. intelligence is a national asset to be conserved and protected and will be shared with foreign entities only when consistent with U.S. national security and foreign policy objectives and when an identifiable benefit can be expected to accrue to the U.S. 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 general limited in duration.[28]

ICD-403 also requires that determinations to disclose or release U.S. intelligence should take into account the professional ability of a foreign intelligence service to protect the classified intelligence from subsequent compromise posing a risk to U.S. national security. However,

> In exceptional cases, there may be a benefit to U.S. interests to disclose or release intelligence to foreign entities under conditions where the recipient's safeguards are likely to be inadequate. In such cases, the anticipated benefits must outweigh the potential damage of a likely compromise.[29]

Intelligence Community Policy Guidance 403.1 (ICPG-403.1) further expounds policy in ICD-403 by providing criteria for disclosing or releasing classified intelligence to a foreign intelligence entity. Its guidance pertains to classified U.S. *intelligence* only, which does not include other classified *information*, such as defense, military, or diplomatic information that is not intelligence. Disclosure or release of classified intelligence is appropriate when it:

- is consistent with U.S. foreign policy and national security objectives;
- can be expected to result in an identifiable, commensurate benefit to the U.S.;
- supports a U.S. diplomatic, political, economic, military, or security policy or treaties; and
- aids U.S. intelligence or counterintelligence activities.[30]

---

[27] ICD-403 defines a foreign entity to include "foreign governments or components thereof; international organizations or coalitions consisting of sovereign states; and others determined by the DNI." ICD-403 also defines "disclosure" and "release." Disclosure is "displaying or revealing classified intelligence whether orally, in writing, or in any other medium to an authorized foreign recipient without providing the foreign recipients a copy of such information for retention." Release is "the provision of classified intelligence, in writing or in any other medium, to authorized foreign recipients for retention." See ICD-403, Foreign Disclosure and Release of Classified National Intelligence, Office of the Director of National Intelligence, March 13, 2013, at https://www.dni.gov/files/documents/ICD/ICD403.pdf.

[28] Para. E.1., ICD-403, *Foreign Disclosure and Release of Classified National Intelligence,* Office of the Director of National Intelligence, March 13, 2013, at https://www.dni.gov/files/documents/ICD/ICD403.pdf.

[29] Ibid., para. E.6.b. An example might be a conscious decision to disclose U.S. intelligence to a traditional adversary government in order to provide warning of an impending terrorist attack.

[30] ICPD-403.1, *Criteria for Foreign Disclosure and Release of Classified National Intelligence*, Office of the Director of National Intelligence, March 13, 2013, at https://www.dni.gov/files/documents/ICPG/ICPG403-1.pdf. ICPD-403.1 also provides criteria for intelligence that is not authorized to be disclosed or released. This includes intelligence that is contrary to U.S. law, or agreements or treaties between the U.S. and foreign countries; concerns a U.S. person (unless collection, retention, and dissemination of such information is authorized by E.O. 12333 and not otherwise prohibited by the Privacy Act, 5 U.S.C. §552(a)); is derived from Grand Jury information under the Federal Rules of Criminal Procedure; or is from a foreign intelligence entity that has not consented to or has explicitly prohibited its further disclosure or release. U.S. intelligence is *generally* not to be disclosed or released if it would reveal intelligence about the recipient foreign entity (unless the intelligence was obtained jointly); or could jeopardize U.S. diplomatic, military or intelligence liaison relationships or activities, or personnel involved in these activities.

An intelligence sharing agreement is often formalized in a memorandum of understanding (MOU) between the U.S. IC element and its foreign intelligence counterpart. There are hundreds of these agreements between the IC and foreign intelligence services. They are not legally binding and are generally classified.[31] This can present challenges for congressional oversight. As one observer of the Intelligence Community remarked, "The near invisibility of liaison arrangements to oversight by elected officials is problematic. Oversight mechanisms have not kept pace with global issues."[32]

For military exchanges that include other types of classified information as well as intelligence, the Department of Defense (DOD) uses General Security of Military Information Agreements (GSOMIA) that detail the level of classification for the exchange and the categories of information that can be exchanged. Whether an MOU or GSOMIA, these agreements provide formal frameworks for intelligence relationships that can be fundamental to broader security relationships (legal enforceability notwithstanding).

Roles and Responsibilities

The DNI has the statutory authority to "oversee the coordination between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means."[33] Assistant DNI for Partner Engagement (ADNI/PE) supports the DNI in carrying out his/her statutory responsibilities, which include:

- Entering into intelligence and counterintelligence arrangements with foreign governments and international organizations;
- Formulating policies concerning these arrangements;
- Aligning and synchronizing foreign intelligence and counterintelligence relationships among IC elements "to further United States national security, policy, and intelligence objectives;"[34]
- Establishing, with the concurrence of departments and agencies concerned, joint procedures to coordinate and synchronize intelligence activities conducted by an

[31] 5 U.S.C. §552(c)(1) governs exceptions to the statutory requirement to disclose to the public meetings of an agency of the government. The provisions of this subsection of the statute cover U.S. intelligence exchanges with foreign partners and the formal agreements that govern these relationships: Meetings of an agency of the government are to be open to public observation,

> "(c) Except in a case where the agency finds that the public interest requires otherwise…[and] where the agency properly determines that such portion or portions of its meeting or the disclosure of such information is likely to-
>
> (1) disclose matters that are (A) specifically authorized under criteria established by an Executive order to be kept secret in the interests of national defense or foreign policy and (B) in fact properly classified pursuant to such Executive order…"

[32] See Richard Aldrich, "Dangerous Liaisons: Post-September 11 Intelligence Alliances," *Harvard International Review*, vol. 24, no. 3 (September 2002), pp. 49-54.

[33] 50 *U.S.C.* §3024(k).

[34] 50 *U.S.C.* §3001, E.O. 12333, *United States Intelligence Activities,* §1.3(b)(4).

> IC element or funded by the National Intelligence Program (NIP), with activities that involve foreign intelligence and security services.[35]

The Director of the CIA (D/CIA) is responsible for implementing the DNI's foreign intelligence engagement policy and coordinating foreign intelligence relationships. These responsibilities are specified in Executive Order (EO) 12333, *United States Intelligence Activities:* CIA has the authority "under the direction and guidance of the DNI … to coordinate the implementation of intelligence and counterintelligence relationships between elements of the IC and the intelligence or security services of foreign governments or international organizations."[36] This authority is reiterated in ICD-310, *Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities outside the United States.*[37]

Overseas, the U.S. ambassador or Chief of Mission is responsible for "the direction, coordination, and supervision of all Government executive branch employees" in a country … who shall be kept "fully and currently informed with respect to all activities and operations of the Government within that country."[38] In other words, the U.S. ambassador has authority over United States intelligence activities within that country. The actual management of intelligence programs and activities in a U.S. embassy, however, falls to the CIA Chief of Station (COS), who is to ensure the Chief of Mission is kept appropriately informed.[39]

ICD-402, *Director of National Intelligence Representatives,* buttresses the CIA's responsibility to coordinate the implementation of policy for the IC's foreign intelligence relationships by assigning to the CIA's Chiefs of Station responsibility as the DNI's representatives in the locations or organizations where they are assigned.[40] In each foreign country, therefore, the COS has day-to-day management and oversight of not only CIA but all liaison relationships by any IC element, with state or non-state foreign intelligence organizations.

Subject to DNI policy and DCI/COS management and guidance, each element of the IC has the statutory authority to conduct relations with foreign intelligence services particular to the

---

[35] 50 *U.S.C.* §3001, E.O. 12333, *United States Intelligence Activities*, §1.3(b)(21).

[36] 50 *U.S.C.* §3001, E.O. 12333, *United States Intelligence Activities*, §1.7(a)(6).

[37] See para. B.3. of ICD-310, *Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities Outside the United States*, Office of the Director of National Intelligence, June 27, 2016, at https://www.dni.gov/files/documents/ICD/ICD%20310%20-%20Coord%20of%20Clandestine%20Human%20and%20Human-enabled%20FI%20and%20CI%20outside%20the%20US%20(27%20June%202016).pdf. Of note, however, there are statutory restrictions on sharing intelligence with the United Nations. Congress restricted the sharing of U.S. intelligence with the United Nations (and any organization affiliated with the United Nations) unless the President certifies to the congressional intelligence and foreign relations/foreign affairs committees that the DNI, "in consultation with the Secretary of State and the Secretary of Defense, has established and implemented procedures, and has worked with the United Nations to ensure implementation of procedures, for protecting from unauthorized disclosure United States intelligence sources and methods connected to such information." The President may waive this requirement by providing written certification to these committees that providing intelligence to the United Nations is in the interest of U.S. national security. See 50 *U.S.C.* §3047 (a)(1)-(2).

[38] 22 *U.S.C.* §3927(1)-(2).

[39] In answers to Director of Central Intelligence pre-confirmation questions, Gina Haspel addressed resolution of disagreements between the Chief of Mission and Chief of Station on intelligence activities: "Intelligence activities that do not have the approval of the Chief of Mission but remain supported by the Chief of Station are referred back to CIA and the Department of State for resolution." *Pre-Confirmation Hearing Questions Submitted to DCIA Nominee Gina Haspel by Senator Ron Wyden (#2) Senate Select Committee on Intelligence, 5 May 2018*, at https://www.intelligence.senate.gov/sites/default/files/documents/aphq-ghaspel-050918.pdf.

[40] See para. G.1.A. of ICD-402, *Director of National Intelligence Representatives*, Office of the Director of National Intelligence, December 23, 2009, at https://www.dni.gov/files/documents/ICD/ICD402.pdf.

element's capability and operational or analytical focus. The National Security Agency (NSA), for example, has the statutory authority to conduct foreign cryptologic liaison relations;[41] the Defense Intelligence Agency (DIA) and military service intelligence organizations have the authority to conduct defense intelligence liaison relationships with their foreign defense or military intelligence counterparts.[42]

ICD-403 specifies the roles and responsibilities of officials making decisions involving the disclosure or release of classified intelligence to a foreign intelligence entity. Each IC element has a Senior Foreign Disclosure and Release Authority (SFDRA), who is a senior official with responsibility for the organization's foreign disclosure and release program. The SFDRA, in turn, designates Foreign Disclosure and Release Officer(s) (FDRO) with the authority to approve or deny requests for disclosure or release of intelligence that originated with that IC element, or coordinate with the FDROs of another organization to request disclosure or release of intelligence that originated with that other IC element and has dissemination control markings.[43] Under ICD-403, the DNI may authorize disclosures or releases of classified intelligence requested by the National Security Council or under circumstances that are not otherwise provided for in policy. The DNI is also the final arbiter in resolving any disputes on what can be disclosed or released.[44]

Foreign Intelligence Service Collection on U.S. Persons

Among the more sensitive aspects of U.S. relations with any given foreign intelligence partner—and of interest to Congress—are instances of any such partner providing to the IC information on U.S. persons.[45] This may occur unprompted as a result of routine collection or a bulk data transfer, or at the request of the United States, subject to approval by specifically designated, trained individuals.[46] In instances when the United States requests intelligence on U.S. persons from a foreign intelligence service, there must be *probable cause* to believe that U.S. persons are involved in terrorism, espionage, other illicit activities, or are themselves the target of hostile foreign intelligence services that may threaten U.S. national security. Counterintelligence collected by a foreign intelligence partner (to support its own internal national security) and shared with the United States that includes information on U.S. persons requires special handling. In these instances, the IC must follow the *Attorney General Guidelines* for implementing *Executive Order (EO) 12333* on properly requesting, obtaining, and handling the information in

[41] 50 *U.S.C.* §3001, E.O. 12333, *United States Intelligence Activities*, §1.7(c)(8).

[42] 50 *U.S.C.* §3001, E.O. 12333, *United States Intelligence Activities*, §§1.7(b)(5) and 1.7(f)(4). This includes the liaison and reporting responsibility of the Defense Attaché Service (DAS) in addition to Service-specific intelligence organizations such as the Office of Naval Intelligence.

[43] ICD-403, Foreign Disclosure and Release of Classified National Intelligence, Office of the Director of National Intelligence, March 13, 2013, at https://www.dni.gov/files/documents/ICD/ICD403.pdf. ICD-403 also specifies the responsibility of disclosure and release decisions to be coordinated with the D/CIA.

[44] ICD-403, E.7.

[45] See, for example, Pre-Confirmation Hearing Questions Submitted to DCIA Nominee Gina Haspel by Senator Ron Wyden (#37) Senate Select Committee on Intelligence, 5 May 2018, at https://www.intelligence.senate.gov/sites/default/files/documents/aphq-ghaspel-050918.pdf.

[46] United States officials authorized to request a foreign intelligence service to provide information on U.S. persons are specified in *Central Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333*, January 2017, at https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf.

order to adhere to privacy and civil liberties protections.[47] Information is authorized and handled according to whether it was obtained by *standard* or *special* collection techniques.

Standard collection techniques involve authorization for an IC element to request, receive, and document routinely acquired information or records on a U.S. person. This can include requests made of a foreign intelligence service for information on U.S. persons *abroad* that exists in their files, or requests of a foreign intelligence service to use their assets to collect information targeting a U.S. person *abroad* using *standard collection techniques*.[48] Officials with the authority to authorize *standard collection techniques* include a Chief of Station, Chief of Installation, or Chief of Base, the Deputy Director of the CIA for Operations (DDO), the Associate Deputy Director of CIA for Operations (ADDO), the Chief or Deputy Chiefs of Operations in a CIA Mission Center, a first, second, or third in command of a DO Division or DO Center, or supervisory personnel who are designed by these officials.[49]

Standard collection techniques may also include occasions when an IC element obtains unevaluated bulk data, such as a hard drive, from a foreign intelligence service that may contain information on U.S. persons collected by routine, unexceptional means. In these instances, "specifically designated officials must document the purpose of the collection activity, how the data was acquired, what steps were taken to limit the collection to the smallest subset containing the information necessary to achieve the purpose of the collection, and further determine how sensitive the acquired data is so that appropriate controls regarding access, querying, and retention may be imposed."[50]

Special collection techniques are defined as techniques conducted *outside* the United States targeting a U.S. person that would require a warrant for the same techniques conducted by the FBI *inside* the United States.[51] They include, for example, physical search, search of nonpublic telephone records, and electronic surveillance. Both the authorization and handling of this kind of information is more restricted than for *standard collection techniques*. *Special collection techniques* require *exceptional handling* as outlined in the *Attorney General Guidelines* implementing *EO 12333*.[52] For authorization of *special collection techniques*—including requests for special collection on U.S. persons by a foreign intelligence service—requests must be forwarded through the agency's General Counsel for concurrence and approval by the Director of

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] See *Central Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333*, January 2017, at https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf. The Attorney General Guidelines implement Section 309 of the Intelligence Authorization Act of 2015, "Procedures for the Retention of Incidentally Acquired Communications."

[51] See *The CIA's Updated Executive Order 12333 Attorney General Guidelines,* January 2017, at https://www.cia.gov/about-cia/privacy-and-civil-liberties/Detailed-Overview-CIA-AG-Guidelines.pdf.

[52] "Unevaluated information subject to routine handling requirements may be treated as if subject to exceptional handling requirements based on policy or prudential concerns." See *Central Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333*, January 2017, at https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf.

> "An official approving the use of a special collection technique directed at a U.S. person outside the United States must document in writing that, under existing facts and circumstances, the official has determined that there is probable cause to believe that the person or entity at whom the special collection technique is directed is an agent of a foreign power, or an officer or employee of a foreign power, and that the information sought is significant foreign intelligence or counterintelligence." [p.17]

the CIA or a designee, the U.S. Attorney General, and, where applicable, the Foreign Intelligence Surveillance Court.[53]

A foreign intelligence partner may provide to its counterpart(s) in the United States intelligence on U.S. persons acquired by *special collection techniques without it being specifically requested* by the U.S. counterpart. This would involve occasions where the foreign partner may want to alert U.S. IC or law enforcement officials of serious counterintelligence concerns in the course of a collection activity employing *special collection techniques* targeting a mutual adversary such as Russia or China. *Exceptional handling* is required when information is collected by *special collection techniques* that involves U.S. persons, and subsequently shared with the U.S., whether or not it is specifically requested by the United States.

Benefits of Foreign Intelligence Liaison

A former member of the Senate Select Committee on Intelligence remarked recently that foreign intelligence services provide the United States some of its most significant intelligence.[54] Two examples are readily apparent. Following 9/11, then-French President Jacques Chirac directed the French intelligence services (the DGSE and DGSI) to share counterterrorist intelligence with the United States "as if they were your own service."[55] Similarly, on September 12, 2001, the day after the attacks, the senior leadership of the British intelligence services (MI5 and MI6) visited their counterparts in Washington, DC, to offer their assistance.[56] The U.S. IC also benefits from intelligence liaison with traditional adversaries, and non-state actors (e.g., Kurdish organizations), on areas of mutual interest.

Intelligence and Information Sharing

Intelligence sharing or collaboration can be defined as "the liaison or collaboration between [intelligence] bodies responsible for the collection, analysis and/or dissemination of information in the field of national security and defense."[57] Sharing *finished* intelligence derived from multiple sources provides less risk of revealing information of any particular source and is thus more typical of many bilateral or multilateral intelligence relationships. The sharing or exchange of *raw* data or *unfinished* intelligence takes place either where there is sufficient trust between partners to provide the necessary security from compromise of collection sources and methods (as there is between the U.S. and Five Eyes partners, plus France, Germany, Norway, and Japan, among others), or it can also occur in situations where there is an immediate need to provide perishable information—such as indications and warning of an impending terrorist attack—that may take precedence over the risk of revealing a source. The exchange of intelligence or

[53] *Central Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333*, January 2017, at https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf.

[54] Remarks of former Senator Bill Nelson, George Mason University Schar School of Policy and Government panel discussion on congressional oversight of intelligence, March 11, 2019.

[55] Dana Priest, "Help from France Key in Covert Operations," *The Washington Post*, July 3, 2005, at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/02/AR2005070201361.html.

[56] Sir Stephen Lander, "International Intelligence Cooperation: An Inside Perspective," *Cambridge Review of International Affairs*, 17:3 (2004), pp. 481-493, at https://www.tandfonline.com/doi/full/10.1080/0955757042000296964.

[57] *Abuse of State Secrecy and National Security: Obstacles to Parliamentary and Judicial Scrutiny of Human Rights*, Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights, Doc. 11907, September 16, 2011, cited in Hans Born, Ian Leigh, Aidan Wills, *Making International Intelligence Cooperation Accountable*, (Geneva: Center for Democratic Control of Armed Forces, 2015), p. 6.

information among the United States and intelligence partners is a daily occurrence treated with great sensitivity. Intelligence sharing may help to corroborate U.S. national sources in addition to possibly providing unique information. Intelligence and information exchanges may involve secure conferencing, phone calls, or, among the closest partnerships, automated data exchange. Attachés belonging to the Defense Attaché Service (DAS) of the Department of Defense or attachés representing other departments, such as the Departments of Justice and Homeland Security, also regularly conduct exchanges with their host-country counterparts.

Indications and Warning (I&W)

Foreign intelligence relationships that provide indications and warning (I&W) of an impending attack or serious threat to the national security of the partner country may take place by means of sharing proprietary intelligence of a partner agency, or collecting intelligence through a joint operation. Among the instances that have become part of the public record are these.

- In 1962, a human intelligence asset of the CIA and British Secret Intelligence Service (SIS, also known as MI6), Soviet GRU Colonel Oleg Penkovsky, provided details of the Soviet nuclear weapons capabilities and nuclear missile sites in Cuba. The information Penkovsky provided during the Cuban Missile Crisis enabled President Kennedy to understand he had three days before the Soviet intermediate range nuclear missiles would be fully operational. It was a warning that the CIA credited as "altering the course of the Cold War."[58]
- In February 2006, GCHQ (the UK signals intelligence counterpart of the U.S. National Security Agency) shared with the United States information from intercepted communications between two Al Qa'ida operatives in Pakistan and the United Kingdom, respectively, indicating their plans to bomb civilian aircraft. Subsequently, the CIA was able to share this information with Pakistan's Inter-Service Intelligence agency leading to the ISI's apprehension of the lead Al Qa'ida planner.[59]
- In 2010, Saudi Arabia, once reluctant to share intelligence with the United States on Al Qa'ida, obtained perishable indications of a sophisticated Al Qa'ida plot to attack cargo planes en route to the United States. The Saudis provided the information to U.S., British, German, and Emirati officials who were able to intercept the bombs and prevent the attack.[60]
- In December 2017, acting on a tip from the CIA, Russia's Federal Security Service (FSB) was able to break up a plot by an Islamic State-linked terrorist cell to bomb Kazan Cathedral and other prominent sites in St. Petersburg, Russia.[61]

[58] "The Capture and Execution of Colonel Penkovsky, 1963," *Central Intelligence Agency: News & Information*, at https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/colonel-penkovsky.html.

[59] See Marlow Stern, "How the CIA Helped Prevent the Next 9/11—and Why You Can't Bring Liquids Onto Planes," *The Daily Beast*, November 24, 2018, at https://www.thedailybeast.com/how-the-cia-helped-prevent-the-next-911-and-why-you-cant-bring-liquids-onto-planes?ref=scroll. The lead planner, Rashid Rauf, later escaped Pakistan's custody, and was subsequently reportedly killed in a U.S. drone strike.

[60] Eric Schmitt and Scott Shane, "Saudis Warned U.S. of Attack Before Parcel Bomb Plot," *New York Times*, November 5, 2010, at https://www.nytimes.com/2010/11/06/world/middleeast/06terror.html

[61] Vladimir Isachenkov, "Putin Thanks Trump for CIA Tip He Says Stopped Bomb Plot," *AP News*, December 18, 2017, at https://www.apnews.com/0531697a83504a3fbc907294551972ba. This example, which received extensive media coverage, also demonstrates how intelligence can be shared between the U.S. and a foreign intelligence service that is more typically an adversary.

Burden Sharing, Expanded Coverage, and Time-Sensitive Contingency Response

Burden sharing, or a division of labor between the personnel and resources of the IC and foreign intelligence partners, is possible with the most trusted, most capable allied intelligence services. The early collaboration between the United States and United Kingdom during the Second World War, which resulted in the success of the Magic and Ultra operations, has continued to the present day with the integration of personnel and burden sharing or "divisions of effort" involving signals intelligence (SIGINT) target areas.[62] The integration is so close that U.S. and British customers/consumers of their products often do not know which country generated the intelligence they are reading/reviewing/consuming.[63] Similarly, U.S. reliance on Japanese signals intelligence coverage of the western Pacific enabled the United States, through receipt of Japanese intercepts of communications between Russian ground controllers and fighter pilots, to pinpoint the cause of the shoot-down of Korean Air Lines Flight 007 in 1983.[64]

Following the end of the Cold War, the United States embarked on a deliberate strategy to benefit from a perceived *peace dividend*. This amounted to relying on foreign partners for intelligence coverage of areas of the world where the United States either did not have access or did not want to expend the resources and effort to establish coverage.[65] Foreign intelligence relationships can provide the benefit of second-hand understanding of issues and areas of the world where the United States may lack national intelligence assets. Moreover, since 9/11, the IC has had to rapidly expand its liaison relationships with state and non-state foreign intelligence organizations for time-sensitive contingency support of fluid counterterrorism operations. Yet there is a risk of over-reliance on foreign partnerships, as a joint congressional inquiry found, when they are not balanced by national intelligence capabilities.[66]

Joint Intelligence Operations

Joint operations may be conducted when the United States and a foreign partner intelligence service contribute complementary abilities in intelligence collection or covert action to achieve a common objective.[67] For example, one partner may be able to provide access to a source of information, and the other the technical capacity to exploit the information for intelligence value. In 1949, at the beginning of the Cold War, the British Secret Intelligence Service was able to tap the communications cables of the Soviet command center during its post-war occupation of

[62] Michael Herman, *Intelligence Power in Peace and War*, (Cambridge: Cambridge University Press, 1996), p. 202.

[63] Sir Stephen Lander, "International Intelligence Cooperation: An Inside Perspective," *Cambridge Review of International Affairs*, vol. 17, no. 3 (2004), p. 487.

[64] Jeffrey T. Richelson, *Foreign Intelligence Organizations* (Cambridge: Ballinger Publishing Co., 1988), pp. 267-268.

[65] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (Washington D.C.: Government Printing Office, 2004), p. 90.

[66] A joint congressional inquiry found that the "peace dividend" of the immediate post-Cold War years relied excessively on liaison relationships with foreign intelligence services at the expense of developing national intelligence capabilities. See U.S. Congress, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* (Washington, DC: U.S. Government Printing Office, December 2002), p. 91, at https://www.intelligence.senate.gov/sites/default/files/documents/CRPT-107srpt351-5.pdf.

[67] Covert action is defined in statute as an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States will not be apparent or acknowledged publicly. 50 U.S.C. §3093(e). See also CRS Report R45175, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief*, by Michael E. DeVine.

Austria. The CIA joined the operation due to its technical ability to read the enciphered messages that the SIS intercepted.[68]

Because of the close link of covert action to national security policy, deliberations over conducting joint covert action operations with a foreign partner may affect U.S. policy decisions and outcomes. In 1953 the British lobbied the Eisenhower Administration for a joint covert action operation that resulted in the overthrow of the elected Iranian government of Prime Minister Mohammad Mosaddegh.[69] Similarly, the British argued against the United States embarking upon covert action in the 1950s to destabilize Soviet bloc governments in Europe.[70]

Basing Rights/Hosting Equipment

Intelligence relations are often part of broader security arrangements with U.S. partners who may provide privileges to base operational and intelligence personnel and equipment in geographic proximity to both the target area and intelligence personnel and facilities of the allied partner.[71] Host-country partners provide political clearance that enables the United States to establish intelligence facilities, and may also provide various degrees of infrastructure support. This has been true of many close U.S. allies, such as Germany, the United Kingdom, Japan, Italy, Spain, Portugal, and South Korea. Other partners that have provided basing rights have risked more politically in doing so (e.g., Turkey, Pakistan, Iran [under the Shah], Iraq, and Afghanistan). During the Cold War, Pakistan permitted the United States to maintain a signals intelligence site in the country, and permitted the CIA to conduct reconnaissance flights from Pakistani airfields. In Iran, in return for significant amounts of military aid,[72] the Shah's government permitted two U.S. signals intelligence sites in the north of the country that enabled the IC to collect missile telemetry from the Soviet missile test facility at Tyuratam.[73]

U.S. intelligence liaison relationships, which expanded significantly after 9/11, included a multilateral facility in France for collaboration on counterterrorist intelligence. Multilateral intelligence sharing—Five Eyes excepted—can sometimes be cited as providing products and services at a level of the least trusted member of the multilateral arrangement. The facility in France, however, which also included representation from the United States, United Kingdom,

---

[68] Jeffrey T. Richelson, *Foreign Intelligence Organizations* (Cambridge: Ballinger Publishing Co., 1988), p. 25.

[69] See for example, Michael Axworthy, *Revolutionary Iran: A History of the Islamic Republic* (Oxford: Oxford University Press, 2013), p. 49.

[70] See Richard J. Aldrich, "British Intelligence and the Anglo-American 'Special Relationship' During the Cold War," *Review of International Studies*, 1998, pp. 340-341.

[71] In 2009 account in *The New York Times,* for example, provides an account of the CIA's covert operation of drones based in Pakistan to target al Qa'ida operatives in North Waziristan during the Obama Administration. See Scott Shane, "C.I.A. to Expand Use of Drones in Pakistan," *New York Times*, December 3, 2009, at https://www.nytimes.com/2009/12/04/world/asia/04drones.html. The U.S. also reportedly, for a time, provided Pakistan with real-time drone imagery and communications intercepts to assist in Pakistan's counterterrorism operations. However, U.S. intelligence officials had been opposed to jointly operating drones with Pakistan and providing advance notice of drone flight operations, believing the information was leaked to militants in the past. See Eric Schmitt and Mark Mazzetti, "In a First, U.S. Provides Pakistan with Drone Data," *New York Time*s, May 13, 2009, at https://www.nytimes.com/2009/05/14/world/asia/14drone.html

[72] See William J. Daugherty, "A First Tour Like No Other: Held Hostage in Iran," *Studies in Intelligence*, Spring 1998, at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/spring98/iran.html.

[73] See Jeffrey T. Richelson, *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology* (Boulder: Westview, 2001), p. 88. Richardson indicates that these sites provided about 85 percent of U.S. intelligence on the Soviet ICBM program.

Canada, Germany, and Australia, underscored the significant level of cooperation by the French in orchestrating counterterrorist collaboration among allied intelligence services to successfully target terrorists outside of Iraq and Afghanistan.[74]

U.S. drone facilities in Djibouti, Pakistan, and elsewhere, have contributed to elimination of certain terrorist threats, and have benefited from support from the host-country intelligence services, despite—in the case of Pakistan—opposition to the U.S. presence by many of the local population.[75] The CIA drone operations in Pakistan successfully targeted members of the Haqqani Network, the Afghan Taliban, and the Pakistani Taliban, among others. From Djibouti, drone strikes have been conducted over Yemen and Somalia with the assistance of the French and permission of the Djiboutian government.

Diplomatic Back Channel

The IC has been used for a diplomatic back channel to foreign governments when there may be few alternatives to reliably communicate important information between heads of state. Generally this involves countries with which the United States does not have diplomatic relations. In these situations, the foreign intelligence services are often closely linked to the head of state and exercise influence similar to that of the foreign ministry. Using intelligence services as a diplomatic back channel may be necessary to convey a personal message, clarify intentions, or diffuse tension. One instance that has become public involves the intelligence ties between the CIA, North Korea's Reconnaissance General Bureau, and South Korea's National Intelligence Service.[76] This channel between IC counterparts, begun in 2009 during the Obama Administration, has been used by senior IC officials to send or receive personal communications between the U.S. President and the North Korean leader.[77]

Risks and Obstacles

There is a variety of risks and obstacles to U.S. intelligence relationships with foreign partners. They result from policy differences, differences in assumptions about a threat, failure to respect human rights, lapses in security, espionage, and legal and informal limits each side may place upon the other. The strongest, most enduring relationships have weathered differences in policy or lapses in security that have led to temporary setbacks in intelligence cooperation.[78] More formidable to overcome are obstacles to intelligence sharing resulting from fundamental differences in values.

---

[74] See Dana Priest, "Help from France Key in Covert Operations," *The Washington Post*, July 3, 2005, at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/02/AR2005070201361.html.

[75] Pakistan, however, has officially denied its Inter-Services Intelligence (ISI) agency closely cooperated with the CIA in conducting drone strikes. CIA drone operations from within Pakistan ended in December 2011 following a strike that killed 24 members of the Pakistani military. See Jonathan A. Landay, "U.S. Secret: CIA Collaborated with Pakistan Spy Agency in Drone War," *McClatchy DC*, April 9, 2013, at https://www.mcclatchydc.com/news/nation-world/world/article24747829.html.

[76] See Daniel Hoffman, "The U.S. Intelligence Mission Targeting North Korea," *The Cipher Brief*, June 12, 2018, at https://www.thecipherbrief.com/column_article/28790.

[77] Michael R. Gordon and Warren P. Strobel, "Spy Channel Paves Way for Nuke Talks," *Wall Street Journal*, January 22, 2019.

[78] Examples include the "Suez Crisis" that resulted in rifts in the special relationship between the U.S. and Britain, and New Zealand's "nuclear-free zone" policy effectively banning nuclear-capable U.S. Navy ships from making ports of call.

Training

Bilateral intelligence training of foreign partners' intelligence services can provide certain advantages to the United States, but can also create noteworthy risks. In its earliest years, the United States, as has been noted, benefited from the assistance of British and French mentors of the fledgling U.S. Military Intelligence Division (MID) during the First World War.[79] Since the CIA's creation, training in intelligence collection and analysis has become a means by which the agency and other IC elements have established and maintained ties to foreign partners. This report cites elsewhere the efforts by the United States to build the German and Israeli intelligence services. Among many other examples of the IC reinforcing strategic ties to foreign partners through intelligence training are U.S. support in training Iran's Ministry of State Security (SAVAK) and Egypt's General Intelligence Directorate (GID). Yet subsequent problems in U.S. relations with these countries and others like them underscore the inherent risks of anticipating the second- and third-order effects of establishing close intelligence ties to fragile and unstable foreign governments.[80]

The Iraqi National Intelligence Service (INIS) provides a similar example of both the benefits and risks of intelligence-training relationships with foreign partners. This organization, established with the CIA's support, was one factor—among others—in turning the tide against the Sunni insurgency of 2004-2008. However, it also became caught up in Iraq's Shia-Sunni sectarian conflict and linked to a proxy fight for influence in Iraq between the United States and Iran. Iran reportedly was involved in an assassination campaign against the Sunni-dominant INIS, 209 of whose officers were reportedly killed from 2004-2009.[81] This was partly a consequence of a rivalry with Iraq's Shia-dominant—and unofficial—intelligence organization within the Ministry of State for National Security, operating under Iran's influence and aligned with Iraq's then-Prime Minister Nouri al-Maliki.

Ethics and Human Rights

Historically, adhering to internationally sanctioned standards for ethics and human rights has challenged the United States IC and its foreign intelligence partners, especially in times of crisis. While the United States can benefit from intelligence shared by authoritarian regimes in the Middle East and elsewhere, these regimes have relatively few restraints against obtaining information by harsh interrogation, or even torture. As articulated by one scholar,

[79] Michael Warner, *The Rise and Fall of Intelligence: An International Security History* (Washington, DC: Georgetown Univ. Press, 2014). pp. 60-63. See also James Igoe Walsh, "Defection and Hierarchy in International Intelligence Sharing," Journal of Public Policy, vol. 27, no. 2 (May – August 2007), p. 167: "British intelligence services provided influential advice and served as an important exemplar during the formative years of the American intelligence community."

[80] Although initially seen as a benefit to cementing a close relationship with the Shah's Iran as a hedge against Soviet influence in the Middle East, long-standing intelligence ties to SAVAK proved to be a significant liability for the U.S. during the 1979 Iranian Revolution and hostage crisis. Close ties between U.S. intelligence and Egypt's GID also proved to be problematic when President Gamal Abdel Nasser sought closer relations with the Soviet Union.

[81] "An Uncertain Future for Iraq's Intelligence Services," *Stratfor Worldview*, January 11, 2012, at https://worldview.stratfor.com/article/uncertain-future-iraqs-intelligence-services. Although experienced members of Saddam Hussein's General Intelligence Directorate (GID), most of whom were Sunni, were represented in the INIS, the leadership of the organization was intentionally chosen for its non-sectarian orientation.

> Authoritarian regimes can employ, among other things, relatively extensive population control measures and invasive intelligence collection methods, can readily obtain information superiority, and are under relatively little pressure to use minimum force.[82]

A lack of control and accountability over an authoritarian foreign intelligence partner employing such methods can undermine the credibility of the information obtained. Political backing for such methods can also produce the same effect. For the U.S., even the perception of engaging in an intelligence liaison relationship with a foreign partner with a poor human rights record can leave the United States vulnerable to criticism. The policy of the IC, as described by a former director of the CIA, is to refrain from exchanging intelligence with regimes that abuse human rights:

> We, the U.S. government, and we, CIA, are very, very clear in terms of the types of behaviors and actions that we will not tolerate …. We, CIA, have not only threatened to cut off relations with some of those liaison partners [when] we have information that they practice [abuses of human rights], we have cut off relations. So I think we need to keep the pressure on them …. The navigation of the shoals that stand between these governments today and a thriving democracy are significant. And I think we have to help them navigate it.[83]

However, the U.S. IC itself has leveraged foreign intelligence partnerships to commit ethical abuses, including the well-documented use of so-called *black sites* overseas. Six days after the 9/11 terrorist attacks, President George W. Bush signed a memorandum of notification (MON) that granted the CIA a number of counterterrorism authorities, including to "undertake operations designed to capture and detain persons who pose a continuing, serious threat of violence of death to U.S. persons and interests or who are planning terrorist activities."[84] Subsequently, DCI George Tenant ordered the agency's Deputy Director of Operations and the Director of the Counterterrorism Center to assume authority for the capture and detention of terrorists.[85] The CIA conducted detentions and interrogations at various secret black sites abroad where CIA personnel, including contract interrogators, employed what has been termed "enhanced interrogation techniques" as authorized by the Department of Justice.[86]

---

[82] Yuri Zhukov, as quoted by Cameron Reed, "America's Best Partner in Middle East HUMINT Needs Help," *Defense One*, June 22, 2017, at https://www.defenseone.com/ideas/2017/06/americas-best-partner-middle-east-humint-needs-help/138889/.

[83] "John Brennan on Transnational Threats to Global Security," *Council on Foreign Relations,* June 29, 2016, at https://www.cfr.org/event/john-brennan-transnational-threats-global-security. Daniel Coats spoke out against the use of torture during DNI confirmation hearings before the Senate Select Committee on Intelligence, February 28, 2017. See https://www.congress.gov/115/chrg/shrg24745/CHRG-115shrg24745.pdf.

[84] *Committee Study on the Central Intelligence Agency's Detention and Interrogation Program (*S.Rept. 113-288*)* (Washington, DC: Senate Select Committee on Intelligence), December 9, 2014, p.11, at https://www.intelligence.senate.gov/sites/default/files/documents/CRPT-113srpt288.pdf.

[85] *Special Review: Counterterrorism Detention and Interrogation Activities, September 2001-Octover 2003* (2003-7123-IG)(Washington, DC: Office of the General Counsel, Central Intelligence Agency), May 7, 2004, p. 3, at https://www.cialgov/library/readingroom/docs/0005856717.pdf.

[86] Memorandum for Alberto R. Gonzales Counsel to the President, Re: *Standards of Conduct for Interrogation Under 18 U.S.C. §§ 2340-2340A,* August 1, 2002 at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB127/02.08.01.pdf; and John C. Yoo, Deputy Assistant Attorney General, *Letter to Alberto R. Gonzales, Counsel to the President,* August 1, 2002, at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB127/020801.pdf. See also *Special Review: Counterterrorism Detention and Interrogation Activities, September 2001-October 2003 (2003-7123-IG),* (Washington, DC: Office of the General Counsel, Central Intelligence Agency), May 7, 2004, pp. 19-20, at https://www.cia.gov/library/readingroom/docs/0005856717.pdf. In 2004, Jack Goldsmith, the successor as head of Office of Legal Counsel (OLC) to Jason Bybee who signed the two memos, withdrew them in 2004.

In its study of the program, the Senate Select Committee on Intelligence (SSCI) reported ten detention sites abroad.[87] Media sources have indicated as many as nine more sites.[88] Although the landmark 2006 Supreme Court ruling *Hamdan vs Rumsfeld* effectively ended the "enhanced interrogation techniques" the CIA employed at the time, and contributed ultimately to the closure of the black sites by 2009, the program proved an embarrassment to the CIA, and complicated the IC's counterterrorism intelligence engagements with foreign partners.[89]

Challenges Vetting Sources, Security Lapses, and Espionage

U.S. intelligence agencies' often long-standing ties to foreign intelligence services have been tested by sharing of uncorroborated information and improper source vetting. Germany and Jordan are close intelligence partners of the United States. Both, however, provide examples of the risk of accepting information or intelligence from partner-controlled, improperly vetted sources.

- The now-discredited information of a German Federal Intelligence Service (Bundesnachrichtendienst or BND) source codenamed Curveball, alleging Iraq was in possession of weapons of mass destruction, influenced the 2003 U.S. decision to invade Iraq.[90] Although the lessons learned from this historic failure to properly vet a foreign intelligence source have reduced the risk of repetition, any intelligence organization can fall victim to accepting unreliable information from an otherwise trusted foreign partner.[91] Further, some foreign partners could

[87] *Committee Study on the Central Intelligence Agency's Detention and Interrogation Program (*S.Rept. 113-288*)* (Washington, DC: Senate Select Committee on Intelligence), December 9, 2014, at https://www.intelligence.senate.gov/sites/default/files/documents/CRPT-113srpt288.pdf.

[88] See, for example, Jane Mayer, "Outsourcing Torture, The Secret History of America's 'Extraordinary Rendition' Program," *The New Yorker,* February 14, 2005. The SSCI report makes multiple references that may indicate detainees were held in other locations. However, the number of redactions in the report makes it difficult to ascertain the exact number of locations that may have served as permanent or temporary detention or processing sites.

[89] Among its findings in *Hamdan vs Rumsfeld*, the Supreme Court determined that detainees were protected by the laws of armed conflict, specifically Common Article 3 (CA3) of the Geneva Conventions. CA3, which governs conflicts "not of an international character," prescribes the humane treatment of detainees or others who have laid down their arms or are otherwise not taking part in hostilities. It prohibits "outrages upon dignity, in particular humiliating and degrading treatment…cruel treatment and torture." See *Geneva Convention Relative to the Treatment of Prisoners of War of 12 August 1949*, p. 91, at http://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.32_GC-III-EN.pdf. For background on CIA ethics education, see CRS In Focus IF10906, *CIA Ethics Education: Background and Perspectives*, by Michael E. DeVine.

[90] For more information on the impact of Curveball, see, for example, John Prados, "The Record on Curveball: Declassified Documents and Key Participants Show the Importance of Phony Intelligence in the Origins of the Iraq War," *George Washington University, National Security Archive Briefing Book No. 234*, at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB234/.

[91] The IC's failure regarding Curveball had several factors which were cited in the Findings and Recommendations of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction: (1) The IC was faulted for relying a single source, Curveball, to support claims that Iraq possessed weapons of mass destruction, despite clear indications prior to the invasion of Iraq that Curveball was unreliable. (2) Senior management at CIA failed to heed warnings by officers in the CIA's Directorate of Operations expressing serious reservations about Curveball's reliability. (3) The Defense Intelligence Agency failed to attempt to validate Curveball's reporting, cited by the Commission as "a major failure in operational tradecraft." (4) Analysts were unable to question their assumptions about Iraq's weapons of mass destruction program despite indications that undermined Curveball's credibility. See Appendix B, List of Findings and Recommendations, p. 558, at https://www.govinfo.gov/content/pkg/GPO-WMD/pdf/GPO-WMD.pdf. The Commission was created by Executive Order 13328, February 6, 2004. President George W. Bush accepted most of the Commission's recommendations that in part directed a efforts to improve intelligence collection and analytical tradecraft. See "President Bush Administration Actions to Implement WMD

render their controlled sources' information unreliable through use of duress or torture.

- In December 2009, a source under control of Jordan's General Intelligence Directorate (GID), Humam Khalil al-Balawi, blew himself up at a CIA facility at Forward Operating Base Chapman in Khost, Afghanistan, killing seven CIA agents. Al-Balawi, who had claimed to be the physician to Ayman al-Zawahiri, then-deputy to Osama bin Laden, was in fact working for al-Qa'ida. At the time, however, he offered the prospect that he could assist the CIA in locating al-Qa'ida's senior leadership. A subsequent CIA assessment of the circumstances that led to the attack concluded that al-Balawi "was not fully vetted" despite having previously provided information to the U.S. and Jordan that had been verified.[92] In a statement outlining corrective measures resulting from the attack, then-CIA Director Leon Panetta determined, in part, that the agency needed to "more carefully manage information sharing with other intelligence services."[93]

The intelligence partnership with Britain has also proven vulnerable to the problems of vetting employees or sources of a foreign intelligence agency. The most notorious instance involved five British graduates of Cambridge University (the *Cambridge Five*), serving in senior positions in MI6 while engaging in espionage as agents of the Soviet Union in the 1940s and 1950s. One of the five, Kim Philby, served for a time as First Secretary (Chief of Station-equivalent) of the British embassy in Washington, DC.

Problems with espionage and violations of security have also affected the U.S. IC. Some close partners have brought U.S. citizens under control as sources for intelligence on the U.S. These include the cases of Jonathan Pollard and Robert Kim spying on behalf of Israel and South Korea, respectively.[94]

Another dimension of the risk to intelligence sharing with foreign partners involves advances in technology. Recently, the Trump Administration expressed concern over the potential decision of a foreign intelligence partner to purchase 5G telecommunications infrastructure that could be vulnerable to penetration by a hostile foreign intelligence service or a company controlled by a hostile foreign intelligence service. The United States Ambassador to Germany, in a letter to the German Minister for Economic Affairs, reportedly warned against Germany purchasing 5th-generation technology (5G) telecommunications equipment from China's Huawei Technologies

---

Commission Recommendations," June 29, 2005, at https://georgewbush-whitehouse.archives.gov/news/releases/2005/06/20050629-5.html.

[92] Leon E. Panetta, *Message from the Director: Lessons from Khost*, posted October 19, 2010, at https://www.cia.gov/news-information/press-releases-statements/press-release-2010/message-from-the-director-lessons-from-khowst.html

[93] Ibid. For a more detailed account of the circumstances that led to the attack on the CIA base in Khost, see Joby Warrick, "Humam Al-Balawi: The Triple Agent," *Newsweek*, June 19, 2011, at https://www.newsweek.com/humam-al-balawi-triple-agent-67873. Despite the policy and operational pressures that ultimately contributed to the failures of intelligence in the Curveball and al-Balawi incidents, it should be noted that a number of U.S., German and Jordanian intelligence professionals expressed reservations about these sources' credibility.

[94] For an account of Jonathan Pollard's espionage on behalf of Israel, see Jeffrey T. Richelson, "The Jonathan Pollard Spy Case: The CIA's 1987 Damage Assessment Declassified," *George Washington University National Security Archive Briefing Book No. 407*, at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB407/. For an account of the Robert Kim espionage on behalf of South Korea, see David Johnston, "Korean Spy Case Called More Serious Than Was Thought," *New York Times*, October 3, 1996, at https://www.nytimes.com/1996/10/03/world/korean-spy-case-called-more-serious-than-was-thought.html?mtrref=www.google.com&gwh=315811738692A70195270F5EF6ADD97A&gwt=pay

Co., suggesting that doing so might require the United States, out of concern for security, to cut back on intelligence sharing between the United States and its long-standing ally.[95] The proposed Intelligence Authorization Act of Fiscal Years 2018 and 2019 (S. 245) would require the head of an IC element entering into an agreement with a foreign intelligence service to consider the vulnerability of the foreign service's telecommunications infrastructure to an adversary of the United States.[96]

Limited Cooperation or Lack of Reciprocation

Limited cooperation or a lack of reciprocation can occasionally afflict even the closest intelligence foreign intelligence relationships. Close partners generally work through these challenges. Policy differences may create more persistent obstacles. Intelligence sharing may be more limited with foreign intelligence services that do not share western democratic values or that have a fundamentally different perspective of the global environment. Non-Five Eyes allies have occasionally expressed frustration with bilateral intelligence ties that are evidently not as close as those of each of the Five Eye countries to the United States. Sometimes these limitations are structural; intelligence sharing agreements (MOUs and GSOMIAs) generally define the limits of what can be disclosed or released. This may result in either partner placing restrictions on what is shared on an issue of mutual national security interest. These structured exchanges may result in overly-general assessments that contribute little to policy-makers' understanding of an issue.[97]

Another limitation affecting cooperation on counterterrorist-related intelligence involves the more restrictive privacy protections of some countries compared to those of the United States. This was true in Europe prior to the terrorist attacks in Paris and Brussels in 2015 and 2016, respectively. European allies' stricter privacy laws prevented their processing and sharing with the United States air passenger name request (PNR) data that could be important to preventing a terrorist attack. Since the attacks in Paris and Brussels, however, the U.N. Security Council (UNSC) and European Union (EU) have partially addressed U.S. concerns by adopting measures to improve tracking and interception of PNR data; these measures are intended to facilitate the sharing of perishable intelligence indicators of terrorist travel.[98]

---

[95] See Bojan Pancevski and Sara Germano, "Drop Huawei or See Intelligence Sharing Pared Back, U.S. Tells Germany," *The Wall Street Journal*, March 11, 2019, at https://www.wsj.com/articles/drop-huawei-or-see-intelligence-sharing-pared-back-u-s-tells-germany-11552314827.

[96] See Section 307, "Consideration of adversarial telecommunications and cybersecurity infrastructure when sharing intelligence with foreign governments and entities" of S. 245, *Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019 (116th Congress):*

> Whenever the head of an element of the intelligence community enters into an intelligence sharing agreement with a foreign government or any other foreign entity, the head of the element shall consider the pervasiveness of telecommunications and cybersecurity infrastructure, equipment, and services provided by adversaries of the United States, particularly China and Russia, or entities of such adversaries in the country or region of the foreign government or other foreign entity entering into the agreement. (https://www.congress.gov/bill/116th-congress/senate-bill/245/text?q=%7B%22search%22%3A%22%5C%22intelligence+authorization+act%5C%22%22%7D&r=1&s=1#toc-H6688A0FF57E34BEDB123B47BFCD4D468).

[97] See Richard J. Aldrich, "British Intelligence and the Anglo-American 'Special Relationship' During the Cold War," *Review of International Studies*, 1998, pp. 345-347.

[98] See UNSC Resolution 2396 (2017) at https://www.un.org/press/en/2017/sc13138.doc.htm. The EU's European Council adopted Directive 2016/681 requiring member states to develop Passenger Name Request (PNR) tracking data systems for flights outside of the EU. See Ambassador Nathan A. Sales, "Counterterrorism, Data Privacy, and the Transatlantic Alliance," German Marshall Fund, July 19, 2018, at https://www.state.gov/documents/organization/284459.pdf.

In situations involving fundamentally different values and assumptions about the global environment, the United States and a foreign partner may limit the intelligence they are willing to share. Describing the long-standing U.S. strategic intelligence relationship with Saudi Arabia, for example, one scholar noted,

> The [Saudi] Kingdom in general was often slow to recognize the threat of terrorism and reluctant to cooperate with the United States. After the 1996 Khobar Towers bombing, the Saudi government did not share vital information with U.S. intelligence. Many of the causes linked to the global jihadist movement, like the fighting in Kashmir and Chechnya, enjoyed wide legitimacy within the Kingdom, and citizen support for these conflicts seemed to pose no direct threat to Saudi security.[99]

In instances where intelligence relations with foreign entities are part of a larger relationship, the benefit to each side might not be directly reciprocated. A foreign partner, for example, may leverage a capability in intelligence, such as human intelligence access to a difficult target, in order to extract benefits from the United States in other areas of the bilateral relationship, such as military assistance.

In one example, Pakistan for years benefited from a relationship with U.S. intelligence that was part of a broader cooperative relationship in defense, counterterrorism, governance, and development. This relationship survived despite strong American objections to indications of Pakistan's support for the Afghan Taliban, Haqqani Network, and other Islamist militant groups, and Pakistan's objections to alleged U.S. violations of its sovereignty. In January 2018 the Trump Administration announced a major policy decision to suspend security aid to Pakistan. Pakistan retaliated by terminating its counterterrorism intelligence cooperation with the United States.[100]

The IC also has (or has had) intelligence liaison relationships with adversaries such as Russia, China, Syria, and Libya. There has been benefit in doing so over a relatively narrow range of mutual interests. However, the apparent benefit of exchanging intelligence with adversaries, such as on counterterrorism, is typically weighed alongside the risks. There is a danger of exposing U.S. intelligence sources and methods to a traditional adversary. Furthermore, intelligence liaison about a particular issue—over time—may risk exposing U.S. sources and methods to the foreign agency, as well as exposing knowledge of corruption connected to that government. Serious policy differences also can reduce or negate the benefits of sharing intelligence. In the case of Syria, both Russia and the U.S. have an interest in resolving the conflict. However, Russia's broader strategic objectives oppose those of the United States.[101]

---

[99] Daniel L. Byman, "The U.S.-Saudi Arabia Counterterrorism Relationship," testimony before the House Committee on Foreign Affairs' Subcommittee on Terrorism, Nonproliferation, and Trade, May 24, 2016, at https://www.govinfo.gov/content/pkg/CHRG-114hhrg20256/html/CHRG-114hhrg20256.htm. This is an historic example. Saudi Arabia has since become a critical intelligence partner against Al Qaeda. As Daniel Byman's subsequent testimony illustrates, "Much changed in 2003, when Al Qaeda began to attack the Kingdom directly…As a result of these attacks, the Kingdom embraced intelligence cooperation with the United States and began to see Al Qaeda as a deadly threat. Despite this level of cooperation, however, Byman cautions, "The United States and Saudi Arabia share many interests, but they do not share common values or a common worldview."

[100] This development received wide press coverage. See, for example, Farhan Bokhari, Katrina Manson, and Kiran Stacey, "Pakistan Halts Intelligence-Sharing with U.S. after Aid Suspension," *Financial Times*, January 11, 2018, at https://www.ft.com/content/59969778-f6b1-11e7-88f7-5465a6ce1a00.

[101] See Steven L. Hall, *Intelligence Sharing with Russia: A Practitioner's Perspective,* (Washington, DC: Carnegie Endowment for International Peace, February 9, 2017, at https://carnegieendowment.org/files/2-14-17_Stephen_Hall_Intelligence_Sharing.pdf. See also Daniel R. Coats, "worldwide Threat Assessment of the U.S. Intelligence Community," January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Over-Reliance on the Capabilities of a Foreign Partner

Although foreign intelligence partnerships may have the benefit of expanding the reach of U.S. intelligence in areas where the U.S. lacks collection assets, they also may pose a risk of the IC relying too heavily on a partner's unique access and capabilities.[102] In the 1970s, the IC's reliance on Iran's SAVAK intelligence organization contributed to the U.S. failure to comprehend developments leading up to the overthrow of the Shah.[103] More recently, Congress, in a *Joint Inquiry* into the conditions leading up to 9/11, the congressional intelligence committees cited the "excessive reliance on foreign liaison services," as a factor contributing to the failure of the IC to develop its own human intelligence sources that could penetrate Al Qa'ida.

> Lacking access to senior, high level al-Qa'ida leadership, the [Intelligence] Community relied on secondhand, fragmented and often questionable human intelligence information, a great deal of which was obtained from volunteers or sources obtained through the efforts of foreign liaison.[104]

The dispersed character of terrorists and terrorist organizations is such that it would be difficult to expect the IC to have an optimal number of U.S.-recruited human intelligence sources in place everywhere they might be needed. There will always be an inherent risk in relying on foreign partners in areas where the United States has not had the time, resources, or capacity to develop its own assets. However, a greater risk was arguably incurred by the U.S. intelligence community in its deliberate, resource-driven strategy of leveraging foreign partnerships during the 1990s.

Conclusion

U.S. foreign intelligence relationships may be easily overlooked in discussions of the importance and inherent risks of cooperation with state and non-state actors in the international community. Little is publicly known about them, in particular how they are structured and how they contribute to U.S. national security. The benefits of these relationships to the United States are weighed against their potential hazards, including outright failure. Congress's role in providing oversight

---

[102] This more commonly describes the risk many foreign intelligence partners have in their relations with the U.S. due to significantly greater resources and capabilities of the U.S. IC compared to those of its allies.

[103] See George C. Wilson, "U.S. Intelligence Expert Misread Extent of Iran Riots, Officials Say," *Washington Post*, November 20, 1978, at https://www.washingtonpost.com/archive/politics/1978/11/20/us-intelligence-experts-misread-extent-of-iran-riots-officials-say/a735c88d-c8f4-4916-a9a3-58172356f300/?utm_term=.3003243fc6fa. The author cites CIA officers who claim that a reduction in human intelligence and covert action in the aftermath of the 1975 congressional investigations into U.S. intelligence activities resulted in the CIA having to rely excessively on SAVAK for information on Iran's domestic developments. The agency did not understand, at the time, SAVAK's interest in shielding the Shah and the U.S. from presenting a more candid assessment of the deteriorating conditions in the country. See also Malcolm Byrne, *Intelligence Reporting on the Iranian Revolution: A Mixed Record*, George Washington University, National Security Archive, at https://nsarchive.gwu.edu/briefing-book/iran/2019-02-11/irans-1979-revolution-revisited-failures-few-successes-us-intelligence-diplomatic-reporting.

[104] U.S. Congress, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* (Washington, DC: U.S. Government Printing Office, December 2002), p. 91, at https://www.intelligence.senate.gov/sites/default/files/documents/CRPT-107srpt351-5.pdf. In this study on the conditions leading up to 9/11, Congress found that the consequent "lack of unilateral (i.e., U.S.-recruited) counterterrorism sources was a product of an *excessive reliance* on foreign liaison services." [emphasis added] See p. 90. The 9/11 Commission described this as a deliberate strategy whose impetus was a perceived need to cash in on a post-Cold War "peace dividend." The CIA could thereby reduce unilateral coverage and place "great emphasis on close relations with foreign liaison services, whose help was needed to gain information that the United States itself did not have the capacity to collect." See National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (Washington D.C.: Government Printing Office, 2004), p. 90.

here is different than its oversight of intelligence in other respects. With the exception of covert action with foreign partners (which is covered by oversight provisions in statute), congressional oversight of U.S. foreign intelligence relationships can be especially challenging due to the passive, low-profile character of sharing intelligence, and Congress's inability to penetrate the internal dynamics of a foreign intelligence service. Nonetheless, these relationships will remain an integral, daily aspect of intelligence activities supporting U.S. national security objectives, and thus Congress has a vested interest in conducting oversight of them.

Author Information

Michael E. DeVine
Analyst in Intelligence and National Security

Acknowledgments

Wil Mackey provided invaluable research assistance in support of this report.

Disclaimer