CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE | THE CHICAGO COUNCIL ON GLOBAL AFFAIRS

TASK FORCE ON U.S. POLICY TOWARD RUSSIA, UKRAINE, AND EURASIA

INTELLIGENCE SHARING WITH RUSSIA: A PRACTITIONER'S PERSPECTIVE

STEVEN L. HALL

Meaningful intelligence sharing is not impossible with the Russians, but the cost is often high and usually not worth the investment.

THE VAGARIES OF INTELLIGENCE SHARING

For those outside of the intelligence business, politicians and everyday citizens alike, the conversation on sharing information with Russia often starts something like this: "Surely there must be *something* on which both sides can agree, *something* that is in both of our common interests on which we can cooperate!" Hopeful suggestions regarding which topics might be shared often follow: What about counternarcotics, child pornography, perhaps even some segment of international organized criminal activity? Certainly, the argument usually goes, counterterrorism seems to be an obvious starting point. But before focusing on the difficulties of sharing intelligence with Moscow and looking at a few recent examples, it is worth better understanding how the U.S. intelligence community actually conducts sharing relationships, and the basic assumptions both intelligence agencies and policymakers have going into such relationships. It is reasonable to expect that two nations, no matter how different their interests may be, should be able to find room to conduct intelligence cooperation on something. This is the bedrock on which the concept of intelligence sharing rests: common interests.

Sharing secrets, however, by definition carries risk. A basic premise of clandestine collection of any type is that the protection of sources and methods is of critical importance, and when one entity shares intelligence with another, it provides a window—sometimes smaller, sometimes larger—on how the information was obtained. The very act of intelligence sharing can sometimes result in the compromise of a source, human or technical, and the cessation of the flow of critical information from that intelligence source. Organizations with which the intelligence is shared, for example, may be able to determine how the information was derived, and may decide to collect it themselves, only to have the target or adversary recognize this new collection effort and shut down access. If the source is a person who is an active member of a targeted organization—say, for example, someone involved in a terrorist cell—they may come under suspicion as their information is disseminated more widely, and information of which only they are aware is acted upon or becomes common knowledge.

ABOUT THE AUTHOR

Steven L. Hall *retired from the CIA in 2015 after thirty years of running and managing Russian operations.*

There are ways to obfuscate the information to protect sources and methods, but policymakers can be understandably worried about this—after all, they want the unadulterated intelligence, and they fear they may be the ones misled. This is part of the natural tension in the intelligence business between collection (which can only occur if sources and methods are protected) and dissemination (which is, after, all the whole point of collection). In some cases, collectors will actually argue against dissemination of intelligence even to the senior-most levels of their own government. Imagine, then, how counterintuitive it can be to share intelligence with foreign governments, much less foreign governments that are hostile toward the United States. Intelligence sharing with foreign services is not a natural act for any intelligence organization. It often takes decades for the intelligence services of even allied countries to become comfortable enough with each other to share sensitive intelligence, and this comfort level is accomplished only when both sides have shown a strong track record of protecting and not abusing the other sides' information.

EVEN MORE COMPLEX: SHARING COUNTERTERRORISM INTELLIGENCE

Counterterrorism information presents a quandary even more challenging than usual for intelligence services, due to the potential impact of terrorist threat information. In many cases, the sharing of sensitive political or other types of intelligence can be carefully weighed and considered before a decision is made as to whether to pass reporting to a foreign government. Thoughtful risk versus gain analyses can be conducted, using both subject matter experts as well as counterintelligence specialists. Certain portions of the reporting can be held back, so as not to reveal the source or how the information was collected. Not so with threat information, where time is usually of the essence, and where each detail may have investigative value. Attacks can be carried out and lives lost in the time it takes to make the assessment as to the pros and cons of sharing.

So terrorism information is treated differently in the U.S. intelligence community. It is a trump card that overrides the normal protections put in place to protect sources and methods in both intelligence and law enforcement, and the normal considerations and restrictions on sharing intelligence are often—quite correctly—suspended. Information is handled at the lowest possible classification level. Reporting is declassified and forwarded to state, local, and tribal officials who are not normally cleared for such information. Intelligence is shared with foreign security services that would normally be considered hostile toward the United States and its allies. This approach is certainly the morally correct one, as it is rarely the case that the protection of sources and methods outweighs saving human lives known to be at risk from an impending terrorist attack. Sharing in such circumstances is of course also politically astute—no Western government would want to pay the political cost of tampering with or holding up threat information, especially if a lethal attack that could have been thwarted was successful as a result. It is therefore difficult to imagine a Western intelligence service willfully allowing a terrorist operation to go forward in order to protect sources and methods, or for political reasons, under almost any circumstances. It would be both morally offensive and politically damaging.

THE RUSSIA PROBLEM

The Russian intelligence services, however, operate under a different set of assumptions regarding both general intelligence sharing and also sharing threat reporting. The Federal Security Service (FSB) and its sister organization, the Foreign Intelligence Service (SVR), as well as the Russian Ministry of Interior and other Russian law enforcement entities, do not find the Western approach to intelligence sharing compelling; in fact, they find it quaint and perhaps a bit naive. For the Russians, information truly is raw power, and sharing it—even inside the Russian government—is viewed first and foremost through a political lens.

Senior Russian intelligence officers have expressed incredulity over the American model, where all-source analysis is conducted using information from across the intelligence community. A Russian intelligence officer once noted, somewhat startled by the all-source approach, "If I did that, my own service would not benefit when we produced really good intelligence. I want to take my information directly to those in power." (It is worth noting that the United States is not entirely immune from the dangers of politicizing intelligence, and there certainly have been cases when this has occurred. Largely, though, it has been done by politicians vice professional intelligence officers. Certainly there is no institutionalization of the use of intelligence to benefit a particular service over another, as happens in Russia.)

Everything, to include the sharing of terrorism intelligence or other types of threat reporting, is part of a much larger, strategic approach to dealing with the United States and the West, and of course there is no political price to be paid in the Russian system for manipulating intelligence when sharing with foreign services. The idea that counterterrorism intelligence can and should be used for strategic gain—even if doing so costs lives—is not unreasonable to the Kremlin. The FSB has undertaken counterterrorism operations in the Caucasus on the thinnest of information—operations that usually end with the "liquidation" of the targets and occasionally their families (Chechen strongman Ramzan Kadyrov, the Russian president's chosen leader in the region, has become particularly expert at this). In Syria, the Russians have assisted in leveling entire population centers, ostensibly to rid the area of terrorists.

This approach is alien inside the U.S. intelligence and national security apparatus, again for both moral and practical reasons. But as Russian officials have told American intelligence officers and national security personnel, we often make a mistake in the West when we impute Western values and methodologies to Russia. Russian intelligence officers, not known for their cultural sensitivity, have noted, half jokingly, that Americans make the mistake of thinking Russians operate in accordance with common Western values. The clear implication is that while Russians *look* European, they do not necessarily *act* European. "You don't make this mistake with the Chinese," one senior Russian intelligence officer once chuckled.

SYRIA AS A CASE IN POINT

Prior to entering into an intelligence exchange with Russia, it bears recalling that a primary geopolitical goal of Russia is to affirm its superpower status as a peer competitor of the United States, and Russia does this by asserting itself at the expense of the United States when it can. Russia's goal of stymying the United States and showing how Moscow can stand up to Washington is sometime facilitated by using intelligence sharing agreements. While Russian President Vladimir Putin and other senior Russian figures often complain that the West is "using Cold War tactics" or "hopes to ignite a new Cold War," at least in the area of intelligence, it is the Kremlin that still operates in a zero-sum-game fashion: a loss for the United States or Europe is a win for Russia, and vice versa.

Syria is a good example of this. Beyond increasing its own geopolitical clout at the expense of the United States and NATO, it is difficult to see what Russia's other interests are in Syria. Certainly they do not include oil or trade, so the most logical answer is that Russia is attempting to reassert its great power status (a very Cold War approach) by exerting diplomatic and military power. (An argument can be made that the Russians want to maintain access to the port in Tartus and establish a military base, but a year-long bombing campaign across Syria argues that there is likely more at stake).

And yet the United States continues to try to find ways to work with Russia, because Russia has positioned itself to be the primary interlocutor with and for Bashar al-Assad's regime in Syria. This is a well-worn Russian tactic: insert yourself into an international situation so that you will have to be

relied upon to help solve it. This approach is aimed primarily at getting Russia a seat at the table, so that the United States and the West cannot act unilaterally. The United States and its allies, in contrast, are actually trying to work with Russia to resolve the situation in Syria, both political and humanitarian. This is a very Western approach, and the Russians see it is quaint, and they know how to leverage it to their benefit.

One mechanism to use in such situations is to take advantage of intelligence sharing, something the Russians know will be attractive to Western politicians. They also know it will come at little to no cost to Russia. Sharing intelligence regarding known terrorist organizations in Syria, as noted above, is commonsensical to the Western mind, especially when Washington and other Western capitals are under increasing political pressure due to the growing humanitarian crisis and other factors to show progress in Syria. Intelligence sharing is also less concrete and less threatening to many policymakers, especially when compared with such measures as arming opposition forces or committing U.S. troops to a war zone. When frustrated U.S. policymakers ask their subordinates what progress is being made with Russia vis-à-vis Syria, intelligence sharing and military coordination (that is, tactical intelligence sharing) can be cited, giving politicians at least the sense of forward movement.

There is certainly no downside to the Russians in sharing intelligence, as they will gain greater visibility into U.S. capabilities, plans, and intentions while not sharing any information that might be harmful to them or their interests. Intel sharing and cooperation—which inevitably involves formal bureaucracies such as Joint Implementation Centers and such—also takes time, another element that works in the Kremlin's favor. Simply setting up and running the sharing mechanisms provides the Russians greater space with which to operate in Syria, buying more time and helping the Assad regime better prepare to act against U.S.-supported anti-regime forces. There is also a concern, not unfounded, that the Russians might pass the intelligence gained from the United States and the West to other governments (Iran, for example), further jeopardizing sources and methods. This is one reason why the U.S. military is reticent to engage in such intel exchanges.

OTHER EXAMPLES

Recent indications that the Russian intelligence services were behind several significant cyberattacks against the United States is another good example of the many difficulties of sharing intelligence with the Kremlin. Twenty-five years ago, intelligence was shared the old-fashioned way: CIA officers would have routine meetings with their foreign counterparts, pass hard copy written memos, discuss a way forward, and then proceed with an agreed-to plan. This time-consuming method makes sharing counterterrorism intelligence dangerously impractical, especially given the speed with which information can and needs to be shared today. Information and intelligence can now be shared much more efficiently via the Internet and other electronic means, but this also exposes Western intelligence agencies to cyberattacks from the very foreign counterparts with whom they are sharing.

The Russians (and in all likelihood the Chinese and others) would not hesitate to use ongoing electronic sharing of counterterrorism information, for example, to penetrate the very networks the West uses to pass the intelligence. For this reason, separate databases and unique transmission protocols must be set up, thereby decreasing efficiency, but increasing security against a cyber intrusion. Again, the West rarely if ever thinks in terms of using counterterrorism sharing as a Trojan horse targeting the Russians: such a proposal would at the very least raise the eyebrows of politicians in Washington, and most likely be deemed inappropriate. The Kremlin would not hesitate.

This was a major concern during the lead up to the Sochi Olympics. Clearly the United States and the international community wanted to do all that was possible to prevent a terrorist attack at the Sochi winter games in Russia. The West wanted to ensure all Olympic athletes, as well as

visiting spectators regardless of national origin, were as safe as possible. That the site of the games was adjacent to the restive Caucasus region of Russia, from where the vast majority of attacks on the Russian government emanate, made the imperative to share intelligence with Russia that much stronger. But the United States was concerned about the traditionally aggressive FSB collection efforts in Russia against U.S. diplomatic outposts and personnel, as well as private American citizens and corporations. This put the United States in a precarious position: if there had been a successful attack in Sochi that could have been prevented if only the United States had not been so cautious given counterintelligence concerns, the moral price and the political fallout would have been significant. The valid counterargument that the Russian intelligence services were no doubt poised to take full technical advantage of any advanced electronics used to more quickly and efficiently share intelligence would have been quickly discredited, despite the validity of the argument. Thankfully, no such attacks occurred.

Given how the Russian government sees intelligence—as a power mechanism for internal political use as well as for informing Kremlin leaders—Russian politics also often complicates and in the end derails meaningful intelligence sharing. For years, the FBI has made good-faith efforts to cooperate with the Russian security services on law enforcement issues that presumably would be in both sides' interest to pursue. Child pornography, organized crime, and cybercrime are good examples, and during the initial stages, joint investigations often go well. Both sides share information, delegations are sent to each others' capitals, and experts and working-level officers collaborate. Often, however, after months and sometimes years of work, the Russian side will suddenly inform the Americans that the joint effort can no longer continue. The FBI is left with the strong sense that the investigation was getting too close to individuals or organizations in Russia with ties to the Russian government. When the Russians understand the direction of the investigation (and if a Russian government insider or other influential party is implicated), they can (and will) warn the Russian target. When the FBI, after a significant investment in time and resources, pushes the Russians, the response is often something akin to, "We will take care of it ourselves from here."

Internal corruption is not the only thing that blocks information sharing on law enforcement operations: the Russians often link external political issues to ongoing investigations. If the Kremlin is unhappy about a U.S. position (say, for example, the Magnitsky bill), Russia will look for what they call "reciprocity," and they will shut down an ongoing area of cooperation. An excellent recent example of this was Putin's suspension of the strategic enriched plutonium agreement with the United States due to his pique regarding Washington withdrawing from negotiations on Syria.

A good threshold when considering how and when to share intelligence with foreign governments is commonality of interest. On a spectrum running from easy and commonsensical to difficult and inadvisable, sharing intelligence with U.S. allies should be (and usually is) on the easy end. Sharing with Russia should be (but sometimes is not) on the opposite side of the spectrum, on the inadvisable end.

It bears remembering, however, that commonality of interest occurs on two levels. The first is when commonality attaches to a specific topic (sharing intelligence on an impending terrorist attack, for example). When the question of whether to share or not is based on a specific topic or situation, sharing with allies is usually obvious, and depending on the specifics, sharing with countries who are U.S. adversaries may also be advisable. But the second, more overarching level of commonality of interests must always be taken into consideration prior to sharing: does the government with whom we decide to share have enough in common with our value system and interests to make the sharing worthwhile? Will the government abuse the intelligence

we share by, for example, making mass arrests, and then incarcerating or killing those who may be innocent without due process of law? Might a corrupt foreign government use the intelligence shared for political purposes, not caring about whether the attack itself is thwarted? Or as with Russia, will a country use the intelligence not just in an attempt to identify and exploit sources and methods but, more dangerously, to advance its own strategic goals? Recall that for Putin, complicating U.S. initiatives serves a purpose—it projects Russia's great power image, as well as Putin's own image as a great leader.

And so while it is easy to exclaim, "Surely there must be some area on which Russia and the United States can agree and share intelligence," as is often the case with Russia, it is much more complicated than that. Russia understands our Western, optimistic, hope-to-share approach, and will use it to what Putin views as his advantage, in a way the United States and the West would find mind-boggling. Especially with terrorist threat information, American intelligence agencies have an obligation to search out new ways to share—even with Russia—but the U.S. government also has an obligation to its citizens not to be naive in this endeavor. Doing so with Russia will result in the serious compromise of national security down the road. Two things at least are true when considering intelligence sharing with Russia: Political expediency and the breathless rush to collaboration comes at a cost. And the ephemeral sense of sharing, while satisfying, can come with a high strategic price tag. The gains rarely justify the risks.

TASK FORCE ON U.S. POLICY TOWARD RUSSIA, UKRAINE, AND EURASIA

The task force will assess the strengths and weaknesses of U.S. and Western policy toward Russia, Ukraine, and Eurasia since the end of the Cold War and offer a set of guiding principles for a durable U.S. policy framework. The task force is a joint effort with the Chicago Council on Global Affairs and is supported, in part, by the Carnegie Corporation of New York.

@CarnegieRussia facebook.com/CarnegieRussia

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance the cause of peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

@CarnegieEndow facebook.com/CarnegieEndowment