Shaking Up The Intelligence Paradigm: Are We Seeking Consensus Without Asking All The Right Questions?

Ronald D. Lee

Efforts to achieve a working consensus about the roles and capabilities of the United States' intelligence community ("IC") form an integral part of broader efforts to reach domestic agreement on the direction of U.S. foreign policy. The IC includes the intelligence organizations and functions of numerous federal government departments, agencies, and services, including the Army, Navy, Air Force, Marine Corps, Central Intelligence Agency, Coast Guard, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Federal Bureau of Investigation, National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), and National Security Agency (NSA). First, the conduct of foreign relations and the pursuit of foreign intelligence both aim to sustain and increase national security and the United States' capabilities to help preserve international stability. Second, the activities and foreign relationships of the IC are themselves part of the practice of statecraft. Finally, the IC directly supports U.S. government officials as they conduct foreign policy. There is no shortage of reports, studies, and commentators proposing that one vision or another of the IC is the vision that should unify the nation. Instead of adding to those gigabytes of insights, this essay summarizes two of the principal lines of discussion and then touches upon two additional challenges for those who study and make decisions about the future authorities and activities of the IC.

FAILURES AND ABUSES, OR SUCCESSES AND FIDELITY TO THE RULE OF LAW?

Much discussion about the perceived woes and proposed reforms of the intelligence community ("IC") proceeds along one of two lines; at times, the discussion moves along both tracks simultaneously.

The first theme is summarized in the two words "Intelligence Failures." This line of discussion posits that the IC has lost its superiority and is no longer able consistently to deliver a decisive information advantage to the nation's policymakers and warfighters. The resulting debate centers on what external and internal factors diminished the IC's capabilities, the potential consequences for United States hegemony, and the measures, cost, and time required to rebuild, recapitalize, and reinvigorate the nation's spies. A series of commissions and studies over the past few years, including the National Commission on Terrorism: Countering the Changing Threat of International Terrorism (2000), have proposed measures to revitalize, reorganize, and reform the intelligence community. The National Commission on Terrorist Attacks upon the United States, an independent commission created by legislation in late 2002, is charged with preparing an all-inclusive account of the circumstances surrounding the September 11, 2001 terrorist attacks and with recommending corrective actions to thwart future terrorist attacks. Most recently, the President of the United States established the Commission in the Intelligence Capabilities in the United States Regarding Weapons of Mass Destruction (WMD) in February 2004 to examine and make recommendations about the capabilities and challenges of the IC to provide intelligence relating to WMD and related threats.

While the first debate inquires whether the IC is understaffed and incompetent, the second debate asks whether the IC is overzealous and malevolent. This second theme is summarized in the words "Intelligence Abuses" and begins from the premise that the IC has strayed from the path of full respect for the constitutional rights and liberties of United States persons before and may stray again. More than a quarter of a century ago, the Church Committee and the Pike Committee of the United States Congress investigated domestic intelligence activities of the IC and proposed reforms, including enhanced legislative and executive oversight, and a statutory framework involving federal judges to regulate the conduct of certain electronic surveillance activities. More recently, the debate has focused on whether the enhanced legal authorities that the IC has received in the wake of the terrorist attacks of September 11, 2001 to collect and share intelligence information should be continued, renewed, or repealed. A full or even a partial discussion and documentation of these enhanced authorities is well beyond the scope of this essay; widely discussed topics include (a) the involvement of criminal investigative purposes and personnel in decisions to commence, alter, or discontinue electronic surveillance and physical search authorized under the Foreign Intelligence Surveillance Act (FISA); (b) the use in criminal proceedings of information obtained pursuant to activities authorized under FISA; and (c) the Federal Bureau of Investigation's investigative powers, when authorized by designated courts, to require any person to produce business records relevant to an investigation concerning international terrorism or clandestine intelligence activities.

Both of these discussions are healthy and necessary, and complementary to each other rather than contradictory. If the IC is not capable enough, it may face temptations to come closer to invading the privacy and civil liberties rights of US persons in order to meet crucial intelligence requirements. On the other hand, arguably the greater the capabilities of the IC to intrude upon the rights of US persons, the greater the need to strengthen scrutiny of the IC's activities. None of this is to cast aspersions on the integrity, intentions, or commitment to the rule of law of the IC and its officials; the IC demonstrates a strong and enduring commitment to the Constitution and the rule of law and has numerous internal and external oversight mechanisms. Rather, these points illustrate the complex dynamic between capabilities and compliance with the legal requirements that protect the rights of US persons.

TWO STRIKING DEVELOPMENTS

Much of both the heat and the light produced by these discussions of capabilities and individual rights have failed to take into account two cardinal challenges to the mission performance and current organization of the IC in the 21st century. This commentary describes those challenges, while leaving for another day proposed solutions or responses to those challenges.

The Size and Shape of the IC. The conduct of foreign intelligence and the receipt and use of its products has always been an inherently federal function. The federal government, of course, is solely responsible for conducting the foreign affairs and national defense of the United States, and intelligence activities derive their primary reason for being from the support of these two activities. The agencies that collect, process, analyze, and disseminate foreign intelligence are federal in charter and international in scope and activities; the agencies and officials that receive and rely upon foreign intelligence are federal and their areas of responsibility are worldwide.

The emerging challenge is occasioned by transnational terrorism targeting U.S. persons and U.S. interests in the United States as well as abroad. As recently as 1997, terrorism and weapons of mass destruction were, according to a statement by President Clinton released by the White House, a priority of the third order, behind supporting military operations and providing political, economic, and military intelligence on countries hostile to the United States. It is reasonable to surmise that the IC now has no higher priority than intelligence to prevent and disrupt terrorist attacks upon the United States, its persons, and its interests. Unlike military operations and intelligence about other nations, intelligence to detect and disrupt international terrorism is not exclusively a federal concern. In recent testimony before the Senate Select Committee on Intelligence, the Director of Central Intelligence George J. Tenet stated, "[F]or the growing number of jihadists interested in attacking the United States, a spectacular attack on the US Homeland is the 'brass ring' that many strive for." The leads, investigative information, and plain old hunches that are needed to formulate specific requirements for terrorism-related intelligence and to inform its collection, analysis, dissemination, and use could well come from state, county, and local law enforcement officers, emergency response personnel, and public health officials as well as from traditional federal generators and recipients of foreign intelligence.

Moreover, because non-federal officials typically have primary responsibility for public safety in almost all areas of the United States, save for areas of federal and tribal jurisdiction, these state, county, and local officials in many cases may have demonstrable needs to receive foreign intelligence reporting. Their involvement and the paramount importance of terrorism-related intelligence reporting, could over time fundamentally change the size, shape, and the operating procedures of what has traditionally been thought of as the IC. Of course some state, county, and city officials already receive some information from the IC and work as informal parts of the IC through ad hoc arrangements and through Joint Terrorism Task Forces (JTTFs).

Both of the debates that permeate discussion about the IC – whether it is doing well or is on the verge of failure and whether it is protecting US person rights or is on the brink of abusing them – could take on substantially different directions in view of the challenges of incorporating non-federal officials into the IC's processes.

The Ambiguity of Identity. A second challenge is the growing ambiguity of identity. It is easiest to discuss this challenge with an analogy to the conduct of law enforcement activities. When local police conduct a physical surveillance or stakeout outside a known criminal hangout, they are watching for the comings and goings of, say, known suspects Person A and Person B. They may also note the presence of Person C and Person D, and will correlate this information with other investigative facts to determine if C and D should be regarded as suspects, victims, or bystanders. In other words, they are putting together facts and attempting to form a coherent picture and investigative story out of those facts; they will in turn use that assessment to direct their further work. The linchpin of this stakeout and assessment, of course, is knowing the individuals' identities; the officers must be able to recognize a specific person as Person A every time they observe that person. Face, hair, body, gait, mannerisms, conduct, and clothes all assist in that recognition of individual identity and individual identity is the anchor around which the investigators build up their analytic picture of the suspects' activities. If Person A could appear to be a different person each time he entered and exited the stakeout location, the analytic picture the police are able to put together would be incomplete and distorted. Conversely, if every person entering and exiting the stakeout location appeared to be the same Person A, the police officers' efforts would also be frustrated.

Now translate this confusion of identities – the target's ability either to change apparent identities constantly, or the ability of several potential targets to take on and use the same identity – to the digital realm. The target may be able to adopt, discard, vary, and multiply electronic identities at dizzying speeds. Moreover, and equally frustrating to an investigator, several different targets, or conceivably thousands or millions of possible targets, could share the same apparent identity. Police officials conducting a lawfully authorized physical or electronic surveillance would confront a fog of confusion and misleading activity not unlike that which a defensive team in football sees when the quarterback executes a double-reverse play and the ball changes hands several times.

As is the case with non-federal involvement in the IC, the myriad possibilities for IC targets to exploit the same ambiguity of identity in the digital age also pose fundamental new issues for the effectiveness of the IC. The ambiguity of identity may also change the terms of debate about the appropriate measures the IC should be able to take, under lawful authority, to conduct its mission while protecting the rights of U.S. persons. One partial response has been the enactment by Congress, as part of the USA PATRIOT Act, of a statute that permits authorized agencies, in seeking judicial approval to conduct electronic surveillance pursuant to the Foreign Intelligence Surveillance Act, to apply for an order that does not limit the permitted surveillance to enumerated communications facilities in circumstances where the court finds that the actions of the target of the surveillance may thwart the identification of that person.

CONCLUSION

Perhaps not since the Church and Pike investigations into the domestic activities of the U.S. intelligence community in the early 1970's has public concern about the appropriate tradeoffs between the authorities of intelligence agencies and the privacy and civil liberties rights of U.S. persons been so spirited. Likewise, the debate about the perceived lack of capabilities of the IC to protect the nation has perhaps never before reached such a high level of intensity because of the stakes. These debates and the search for a working middle ground are healthy and necessary activities for a democracy, and prerequisites for a non-partisan consensus on foreign policy.

As these debates proceed, they should be informed by careful attention to two relatively recent developments: the need somehow to involve state and local officials as appropriate in the intelligence requirements, generation, and consumption cycle; and the need to deal with the ambiguities of digital identity. These developments may require rethinking key foundational assumptions on which the IC has operated for the past half-century or more. After this careful reexamination, which may help to determine the success of the community in protecting the nation against global threats, the search for consensus on the appropriate level of the IC's capabilities and legal authorities can and should resume with renewed vigor and insight.

Ronald D. Lee, a partner at Arnold & Porter LLP in Washington, D.C., focuses on national security and technology law and policy. He has served as the General Counsel, National Security Agency, Chief of Staff to the Director of Central Intelligence, and Associate Deputy Attorney General, U.S. Department of Justice. The views expressed in this article are his own and do not necessarily represent the views of Arnold & Porter LLP or its clients. The author would like to thank Margaret A. Hamburg, M.D. and Tod Cohen for discussions that contributed to this article.