III. Special Correspondences

Watchlisting

by Kenneth Duncan

Abstract

Watchlists have become a vital component of any country's counterterrorism strategy. As first developed over three decades ago in the United States by a far-sighted analyst in the Department of State, watchlisting functioned primarily as a means enabling all-source intelligence to be used for the purpose of excluding terrorists and others from entering US national territory. Today with the rise of domestic terrorists, such watchlists must be inclusive of all potential and real terrorists, including those from the growing category of every country's own citizens.

Keywords: watchlisting; watchlists; TIPOFF; terrorist lookout systems; intelligence sharing; profiling

In early 2016, the Dutch government, when holding the rotating chair of the European Union, noted that the absence of common standards between EU governments diminished the impact of information sharing and this in turn undermined the effectiveness of the EU's terrorist watchlist.[1] As a remedy for this situation, the Dutch authorities proposed adopting 12 criteria under which EU member states would agree to share their information on terrorists with the help of a common watchlist. Agreeing with the Dutch conclusion, the UK government viewed the current situation as compromising British security by facilitating the travel of terrorists.[2]

Before we are too critical of the EU's problem, however, we should remember that in today's world sovereignty still matters. Individual states within and outside the European Union are entitled to approach the definition of terrorism from the perspective of their own history, policy, and legal systems. And so as the old cliché would have it one man's terrorist is (still) another man's freedom fighter or, to put it another way, it all depends upon which end of the gun you are looking at. For the current perspective we need look no further than the Kurds. To coalition forces fighting ISIS in Iraq and Syria they are valued allies; to the Turks facing a renewed Kurdish bombing campaign against Turkish civilians and security forces they are terrorists. Indeed it was not too long ago that the EU itself was at odds with the US and Israel over whether to consider Hizballah a terrorist as well as a political organization. And during the Iran/Contra Affair of the 1980s, the US for too long refused to accept that the Iranian government with which it was negotiating the release of US citizens was actually controlling their Hizballah captors and was therefore a state-sponsor of terrorism.[3] In these cases the terms terrorism and terrorist were seen as pejoratives useful for condemning those organizations one opposed or labels to be avoided when the political consequences of too rigorous an application would compromise other diplomatic initiatives.

Yet even if we set aside this definitional question, there are other problems with watchlisting terrorists. To understand them in context, we must first look at how watchlisting works. Through an accident of professional employment, I have been acquainted with watchlisting ever since 1987 when an analyst in the Department of State's Bureau of Intelligence and Research (INR) created the US government's first all-source terrorist database (watchlist) to support the decision-making of consular visa officers overseas. One of the War on Terror's unsung heroes, John Arriza, first solved the problem of how to marshal the secret intelligence on terrorists held by US intelligence and law enforcement agencies in aid of consular officers overseas. Thanks to his efforts, from 1991 onwards US immigration officials at ports-of-entry were able to detect terrorists attempting to enter the US. And so over a decade before the 9/11 Commission highlighted the dysfunctional nature of intelligence sharing on terrorists and recommended the transformation of intelligence sharing from

a 'need-to-know' to a 'need-to-share' basis, John Arriza had solved this problem.[4] In doing so his program, known as TIPOFF[5] grew from a shoebox holding index cards to an electronic database that contained 130,000 names and aliases contributed by 104 US government agencies as well as several foreign countries.

TIPOFF, like any watchlist, was actually a system involving three key functions:

(i) data collection on suspicious individuals;

(ii) the processing and storage of this data in a secure environment combined with a robust capability for finding individuals quickly and accurately; and

(iii) the sharing of results beyond the secret world of the intelligence community.

Each function is fraught with problems. To begin with, rarely in any system would all three of these functions be performed by the same agency and so underlying each function is the need for trust between and among the system's component organizations–contributors, processors, and end users. Above all, contributors must trust that their sources and methods will be protected so that informants, technical systems, or ongoing operations will not be compromised. Paramount in protecting this information is a secure method of transmission, storage, and dissemination. Contributors must also have trust that their intelligence/information will only be disseminated and used with their permission. This is not only to protect sources and methods but also to ensure that 'operational leads' provided by one agency will not be 'poached' by another as can and does happen between competing law enforcement agencies at times or between intelligence and law enforcement agencies due to their differing agendas.

This trust must extend further so that even the declassified elements such as the names and related biographical information of terrorists will not be compromised by being made too widely or too openly available so that terrorist organizations would be alerted when the identity, aliases, or affiliation of their members were known. There must be trust too that the irreducible risks in providing this intelligence/information is justified because the system will be able to detect and take action against the terrorists contained in its database while still protecting the secrets that underlie that action. Such trust is even more difficult to achieve when the sharing of this information is between states, for then there must be trust in the professional competence of each state's respective services and that their security policies are in general alignment. What level of trust for sharing information on Hizballah terrorists, for example, could be placed in the Lebanese government when Hizballah itself was a member of that government?

TIPOFF was a trailblazer in all of these areas. Because TIPOFF was located in the State Department's Bureau of Intelligence and Research (INR–one of the key elements of the US Intelligence Community), it had access to all-source intelligence as well as diplomatic reporting and open source material. TIPOFF was able to gain the cooperation of both intelligence and law enforcement agencies by adhering strictly to the principle that the originator retains control of the data it provided throughout the process. Yet even so cooperation was not automatic or seamless. Until the terrorist attacks of 9/11 highlighted the need to make terrorist watchlisting a priority in order to prevent future terrorist attacks from happening even at the risk of compromising sensitive information, TIPOFF had to rely upon the willing cooperation of providers such as CIA's Counterterrorist Center, whose mission was to pre-empt, disrupt, and defeat terrorists, and the FBI, whose mission was to arrest and prosecute terrorists. For neither organization was watchlisting terrorists a core function and therefore neither was it a priority.[6] Rather, in pursuit of their specific agendas, most agencies were supported by their own databases; hence there was one for al Qa'ida, one for Hizballah, and another one for Hamas etc.

The history of Nawaf al Hazmi and Khalid al Midhar, two of the terrorists who hijacked AA Flight 77, is illustrative of the pre 9/11 situation. CIA identified both terrorists in January 2001 when they were attending an al Qa'ida meeting in Malaysia. Yet their identities were not sent to TIPOFF for watchlisting until August

21, 2001. As a consequence al Midhar obtained a US visa at the US Consulate in Jeddah on June 13 and both entered the US in July.[7]

Nor at the time was TIPOFF intended to be a comprehensive list of all terrorists. This was because the purpose of any watchlist determines its composition. The purpose of a border-security watchlist, such as TIPOFF, obviously is to prevent terrorists from entering the US. Consequently, while TIPOFF did contain information on terrorists from all regions, it was not authorized to enter into its files US citizens or alien residents since both had a right to enter the US and, in any case, the Intelligence Community was not authorized to collect or store information on US citizens. Sharing terrorist information with other countries at that time also was conditioned by their own legal restrictions on the possession of data for their citizens as well as their differing definitions of terrorists and terrorism. Hence TIPOFF was not able to pass information on nationals of the receiving state, nor would that state pass information on US citizens to TIPOFF. This limitation was not resolved until after the 9/11 attacks when TIPOFF's successor system's role was transformed from border-security into counter-terrorism.

Storage and retrieval of terrorists' identities was and remains problematic too. Who to enter requires a template for managing the degree of certainty about an individual's identity and activities. When John Arriza created TIPOFF, there was no such universal template for the USG. So he used definitions contained in the report of the Vice President's (George H.W. Bush) Taskforce on Terrorism and that yielded three categories: reasonable suspicion, reasons to believe, and beyond reasonable doubt.

Reasonable suspicion was just that, a suspicion, and not considered grounds for action should the person trigger a 'hit' in the system. It was a placeholder until further information came along or for consular or immigration officers to ask for further proof of the person's bona fides. Using this criterion, Hamadam al Shalawi was entered into TIPOFF after he twice attempted to enter the cockpit of America West flight 90 on 19 November 1999. This was sufficient to trigger a name check when he applied in Riyadh to renter the US on 5 August 2001. His visa was denied on 7 September 2001. According to the 9/11 Commission Report, the FBI suspected that this was a dry run for the 9/11 attacks.[8] Reason to believe was based upon a higher standard and in visa application cases probably would be sufficient to deny the person a visa. Proof beyond reasonable doubt could take many forms, including conviction for terrorist offences, known membership in a terrorist organization, direct evidence of fundraising or recruiting for terrorist organizations, or inciting terrorist attacks.

Aliases are an obvious problem but one that is relatively straightforward: you either know them and the true identity behind a name or you do not. Naming conventions differ by region, custom, culture, and religion and are far more complex. The popularity of certain names such as Mohammed for Muslims or Jesus and Maria for Hispanic Christians can make finding the one from many difficult; a problem compounded when some cultures can only use one name as occurs in Afghanistan. Hispanic patronymic and matronymic conventions are another problem. Equally troublesome is sorting through various versions of anglicised names from Persian, Arabic, Chinese and many other languages – there are over 50 anglicized versions of Muammar Gaddaffi for example. One solution employed by TIPOFF was an early computer algorithm that assigned numeric values to names to aid in sorting through this mire. Now we have biometrics coming increasingly to the fore as a means of fixing identities regardless of name confusion or aliases.

TIPOFF was able to put the highest levels of classified material at the service of border security by selectively declassifying only the minimum information necessary. Normally this was the name and sufficient identifying data to enable a consular or immigration officer to be aware that the USG held more information about the individual.[9] Even such limited information as this was only declassified and released with the approval of the agency that provided it. Likewise after a 'hit' was obtained, the providing agency always had to approve any further action based upon its classified information. Consular and immigration officers in the

field were instructed by Washington on what action to take but were not told the secret information on which these instructions were based.

In every case the TIPOFF system attached supporting documentation to each file. This was crucial because the highest classification level of the documentation established the classification level of the entire file. Such a precaution was essential in preventing the accidental disclosure of information about a terrorist that might compromise sources and methods. Electronic attachment of the documentation, when possible, also made the entire knowledge base immediately accessible and eliminated the risk of lost paper files. This documentation established which agencies were the 'owners' of that information and so needed to be contacted should the name trigger a 'hit.' This was absolutely essential when a suspected terrorist was standing before an immigration office at a US port of entry and TIPOFF needed to coordinate a positive identification and an immediate decision on his or her admissibility. This normally involved conversations with the agencies that had provided the documentation to obtain their permission and then releasing this information to an immigration supervisor who was cleared by the intelligence community to receive it. That immigration supervisor then instructed the port of entry on the disposition of the suspected terrorist.

TIPOFF today no longer exists. It and its functions were assimilated initially by the Terrorist Threat Integration Center (TTIC), later by the National Counterterrorism Center (NCC) and The Terrorist Screening Center (TSC). But in its history, John Arriza and TIPOFF were confronted by and found solutions to problems that continue to affect such programs today. Its role has changed as a result of this assimilation. The terrorist attacks of 9/11 demonstrated that the threat was ubiquitous–terrorists could plan operations on one continent, fund them from resources obtained on another, and prepare and execute them on a third. To counter such a threat, a border-security watchlist was no longer sufficiently comprehensive. Counterterrorism watchlists now must be inclusive of all terrorists, including the growing category of every country's own 'homegrown' terrorist citizens. The Terrorist Identities Datamart Environment, as the current compendium of terrorists is known, now has over 25,000 US citizens among its 1.1 million entries. It is maintained by the NCC and used to populate the FBI's Terrorist Screening Database and its No-Fly list.[10] Yet it still adds people to the list using categories, such as reasonable suspicion, pioneered by TIPOFF. And the broader mission is the same: to bring together all-source intelligence and use it to go after terrorists around the world.

About the Author: **Kenneth Duncan,** *Ph.D., is a retired US Senior Foreign Service Officer and former Senior Adjunct Professor of Terrorism in the Program on Terrorism and Strategic Studies at the George C. Marshall European Center for Strategic Studies.*

Notes

[1] Extremists free to travel to UK because EU states cannot agree on the definition of a 'foreign fighter,' *Daily Telegraph*, 23 April 2016.

[2] Ibid.

[3] David C. Martin and John L. Walcott, Best Laid Plans: The Inside Story of America's War against Terrorism. New York: HarperCollins,1988, p. 360.

[4] The 9/11 Report. The National Commission on Terrorist Attacks Upon the United States. Thomas H. Kean, Chair, and Lee H. Hamilton, Vice Chair. Official Government Edition. Washington, DC.: Superintendent of Documents, 2004.(ISBN: 0-16-072304-3); Recommendation 13.2: Unity of Effort in Sharing Information.

[5] Not the least of John Arriza's accomplishments was breaking with the annoying habit the US government and military have in reducing everything to an acronym. Refreshingly TIPOFF was not an acronym for anything; it was instead an apt descriptor of its mission.

[6] According to TIPOFF data, CIA and the State Department were the major contributors, followed by NSA. The FBI was the predominant law enforcement provider.

[7] The 9/11 Commission Report, op.cit (note 4); Chapter 8 details their travels and belated US efforts to catch them once they were in the US. See also History Commons – Complete 9/11 Timetable; URL: http://www.historycommons.org/project.jsp?project=911_project .

[8] The 9/11 Commission Report, op. ict., p. 521.–The FBI assessment was cited in footnote 60: "After the 9/11 attacks, FBI agents in Phoenix considered whether the incident was a "dry run" for the attacks."

[9] This information usually comprised the date and place of birth, nationality and passport number when known. More recently biometrical data are also used by the system.

[10] Alan Fram. 'Why can people on the terrorist watchlist buy guns and other FAQs'. *Associated Press,* June 14, 2016.