Chapter 20

The Role of Intelligence in the Prevention of Terrorism (Early Warning – Early Response)

Kenneth A. Duncan

This chapter outlines how intelligence has adapted to the ever-changing threat of terrorism, and the crucial role "warning" has played and will continue to play in countering and mitigating this threat. To better understand warning's capabilities and limitations, it also explores the nature of intelligence as well as the factors underlying warning's collection, analysis, production, dissemination, and reception. It traces the relationship between intelligence and law enforcement agencies as it evolved as part of the US government's organizational response to terrorism from the late 1960s onward, highlighting both its strengths and weaknesses. Finally, it discusses problems arising from the often-troubled relationship between intelligence producers and consumers – from policymakers to the general public – which can lead to obstacles in turning an early warning into an early response.

Keywords: 9/11, early warning, homeland security, intelligence, prevention, public warning, TIPOFF, United States.

"The terrorism threat is constantly evolving in response to social, political, and technological change, as well as adapting in response to counterterrorism pressure'.
Daniel Byman [1]

Introduction: Understanding Intelligence

At the main entrance to CIA's headquarters building in Langley, Virginia. is an inscription from the Gospel of St. John: "The truth shall make you free," which reflects Intelligence Officers' belief that their role is to "speak truth to power."

But contrary to this common view regarding intelligence assessments, nothing could be further from the truth. Intelligence and warning are not about the objective truth at all. Instead, they are about probability, or as former CIA Director Michael Hayden put it, "If it is a fact, it ain't intelligence."[2] Precise information such as that obtained in 2010 about bombs concealed in photocopier cartridges airmailed by Al-Qaeda in the Arab Peninsula (AQAP) is rare and is not a warning at all, but actionable intelligence.[3] To obtain it, an intelligence service or police department has to be, not only very competent, but also very lucky. An intelligence-derived warning is merely about assessing the threat potential of various terrorist groups and, more recently, often of individual terrorists and proto-terrorists. In this respect it resembles the intelligence community's (IC's) role in producing indications and warning (I&W) during the Cold War to warn of evolving military threats.

There is a basic difference between the two, however. Terrorist threat warning is the mirror image of I&W. During the Cold War, however, both NATO and the Soviet Union were better at assessing each other's respective military capabilities than they were at understanding their opponent's intentions. To illustrate this, in the early 1980s, the Soviet Union misinterpreted President Reagan's 'Evil Empire' rhetoric as preparatory to a nuclear attack.

In contrast, terrorists are not reluctant to share their general intentions to attack us - their numerous threats by audio, video, and internet leave us in no doubt about that.[4] What we are less well informed about is the relationship between intentions and capabilities to carry out specific attacks. When Al-Shabaab, a Somali-based terrorist group, produced a video calling for attacks on Oxford Street shops in the UK and the Mall of the Americas in the US (among other targets), they were "publicly calling for independent actors in their homelands to carry out attacks," but they were not believed to be capable of sending their own terrorists.[5] No one knew who was listening or motivated by this.

---

[1] Byman, Daniel, cited in Hoffman, Bruce, and Ware, Jacob, 'The Challenge of Effective Counterterrorism Intelligence in the 2020s', *Lawfare (blog)*, 21 June 21, 2020; Available at: https://www.lawfareblog.com/challenges-effective-counterterrorism-intelligence-2020slawfareblog.com .
[2] Cited in Petersen, Michael, 'What I Learned in 40 Years of Doing Intelligence Analysis for US Foreign Policymakers', *Studies in Intelligence*, Vol 55, No. 1., March 2011, p. 3.
[3] 'Yemen parcel bomb was 17 minutes from exploding', *BBC*, 4 November 2010. The two bombs were discovered after a Saudi tip-off.
[4] See for example Osama bin Laden's March 1998 *fatwa* against the US or his interview with CNN in March 1997. The Foundation of the New Terrorism (Chapter 2), *The 9/11 Commission Report*, New York: W.W. Norton & Company, 2004, pp. 47 ff.
[5] Whitehead, Tom and Peter Foster, 'Al-Shabaab calls for attacks on Oxford Street and Westfield centres in new terror threat', *The Telegraph*, 22 February 2015.

DOI: 10.19165/2020.6.0120

In intelligence parlance, terrorism is a hard target. It is one of those awkward issues – international organized crime and the proliferation of weapons of mass destruction are others – that are not and never were problems exclusively for intelligence or for law enforcement or for diplomacy, or for the military for that matter. Unlike military forces, terrorists do not have armored divisions, intercontinental ballistic missiles, an air force or navy, which negates much of the IC's capabilities, themselves legacies of the Cold War. Satellite images, for example, of a vehicle loaded with explosives looks like all the others on the streets of Baghdad, Kabul, Cairo or anywhere else in the world.[6]

Terrorist units are usually small and often comprise nothing more than a group of friends or even a single individual who self-radicalized - the increasingly common lone-actor phenomenon. Incidentally, both former US and Soviet intelligence officers agree that most spies self-present themselves to intelligence services; they are volunteers and have not been recruited. Terrorists are less likely to turn on their co-defenders, due to their high level of commitment and the close connections to other cell members .[7] This new generation of terrorists may not have any meaningful direct connections with any known groups, which makes detection of these smaller groups even more difficult.t

Warning: Its Nature, Role, and Mechanics

Warning begins with intelligence. which is usually secret and, therefore, not available to anyone without 'need to know' and proper security clearances. After all, why would anyone declare something 'secret' if they wanted to share it indiscriminately? In large measure the IC commonly classifies intelligence, that is, declares it to be secret and restricts access to it, in order to protect its method of acquisition – known in the trade as "sources and methods."

The important point to remember about protection of sources and methods is that it is not a reflection of the veracity of the intelligence. To classify intelligence as Top Secret is not a declaration that it is twice as reliable as Secret intelligence is not necessarily more reliable than public statements or other open-source material, such as news reports. The chief of the intelligence service of a foreign country might tell the CIA in confidence about corruption in his government or he might make an open declaration of it in a local newspaper. His information might be true or false but one cannot judge that by its intelligence classification. This was not such a problem during the Cold War when the universe of those involved was relatively limited. To return to the example of satellite imagery; apart from photos of ubiquitous cars and trucks, military hardware is often hard to disguise. Soviet jet fighters, for example, were usually shipped disassembled in crates and since each type of aircraft had its own unique crate, analysis of a crate's image ("crateology" as it was called) revealed which type of fighter aircraft it contained. Furthermore, finished intelligence of this nature, when disseminated to key military, intelligence, and policy customers, was comprehensible for its consumers because all understood the reliability of the technical intelligence and its limitations with regard to guessing the underlying intent.

[6] Aerial photographs can sometimes be useful after the fact. After the 1984 suicide bombing in the US Embassy in Lebanon, satellite photographs showed tire-tracks around obstacles representing the Embassy's security barriers at the Sheikh Abdallah barracks in Baalbek; that helped fix responsibility with Iran and its terrorist surrogate Hezbollah. Martin, David C. and John Walcott, *Best Laid Plans*, New York, Harper and Row, 1988, p. 159.

[7] Related by former KGB Major General Oleg Kalugin in conversation with the author.

DOI: 10.19165/2020.6.0120

Consider what happens with terrorism intelligence when those with "need to know" includes the broader domain of homeland security: law enforcement, crisis management, crisis response, border security, and regulatory agencies. It goes still further into the universe that lies outside the US Federal Government, such as state and local health officials, state and local police, private corporations, and increasingly the general public, few of whom are able to see secret information or are used to understanding the nuances of intelligence products.[8] New customers require new forms of information, ranging from guidance on potential threats to critical infrastructure, to terrorist names and identifying data for watchlists. As it is not possible to share everything to everyone, effective sharing requires a new paradigm in order to ensure that everyone has access to the information necessary to perform their duties.

This brings us to the often-overlooked, yet critical element in intelligence preparation: the analysis. As noted above, intelligence, especially warning, begins where the truth leaves off. The analyst's role is to transform raw intelligence, including verified information, such as the movement of terrorists or transfer of their funds, into finished intelligence and warning products. In doing so, it provides insight into, and possibly understanding of, an event, a situation, or the intentions and/or capabilities of an adversary. but this is not the same thing as the truth. In the words of one of CIA's veteran analysts:

> "The business of intelligence analysts is more about putting facts in perspective. … Sources – clandestine, open source, technical, diplomatic etc. – are not the same as knowledge. Sources are not the equivalent of, or a substitute for expertise. … All sources are best thought of as opinions, some more authoritative than others, but all should be subject to careful reflection and comparison to what we know and believe."[9]

What are a particular terrorist group's tactics and targets likely to be? These are the questions analysts can address but cannot answer definitively as they transform raw intelligence into finished intelligence and warning products. Almost always there is an underlying ambiguity, which can be seen as the fundamental difference between intelligence and information.
With this in mind, we can now review the role warning plays in the state's response to the challenge of terrorism.

Aiding the Allocation of Resources

Deciding where to allocate resources in a risk-based part of a counter-terrorism strategy. Countering terrorism is a resource-heavy undertaking in which no country has the ability to protect everything. Guided by warning assessments, security services can allocate their resources to protect individuals, groups, and locations (e.g. embassies, government buildings, and airports) which are at the highest risk.[10] With sufficient time and threats of sufficient magnitude, warning might also be used to obtain funding for additional security resources.

[8] MI5 provides a publicly accessible website on terrorist threats. Available at: *mi5.gov.uk* and *gov.uk>terrorism-national-emergency*. The State of Connecticut uses a reverse 911 calling system in order to disseminate emergency information to the general public. Available at: *ct.gov/CTAlert*.
[9] Peterson 2011, p. 4
[10] Palombi, Simon, ''Known to Police': Assessing Terrorism Risk', *Chatham House Expert Comment*, 18 March 2015. Available at: Chathamhouse.org/expert/comment.

DOI: 10.19165/2020.6.0120

The disruption of terrorist plans from warning can come about by deliberately alerting terrorists that their plans have been uncovered. Besides simply announcing publicly that a plot has been discovered, heavy-handed surveillance of known terrorists or their supporters is a more subtle option. Warning-led additional security measures, such as the installation of security barriers or changes in security operating procedures could delay the terrorist's, or might even persuade them to abandon or delay their entire operation. This would give police and intelligence services more time to neutralize the group. Consequently, when a predicted attack fails to take place, rather than an indication of a failure of warning, it may have been the result of successful, warning-induced countermeasures. This is hard to gauge, however, because it is often difficult to determine if the intelligence was accurate or whether the terrorists were engaging in a form of bluff to keep the authorities on edge. For these reasons, it is seldom possible to fully quantify the effectiveness of specific warnings in these circumstances to the public, security services, and especially to Congress.

Pre-emption of terrorists can occur through so-called premature arrest, that is one based on warning assessments before enough evidence for a successful prosecution has been acquired. Even if the terrorists are ultimately released, the arrest or detention itself often is enough to disrupt the plan and should be considered as a successful counter-terrorism operation. Similar to disruption, given that the stakes in a successful terrorist attack are so great, it is no longer possible for law enforcement agencies to risk an attack by delaying action until the last minute in hope of acquiring further evidence. After 9/11, the FBI took this message on board and changed its priority from prosecution to pre-emption (see the Post-9/11 Responses section for an extensive analysis hereof).

Mitigation of terrorist attacks are made possible when governments are alerted to the possible nature of the attack. Armed with such knowledge, they can take additional security measures to enhance the detection of terrorists or to make it more difficult for terrorists to enter or approach potential targets. Installation or repair of security screening equipment, such as scanners at entrances, surveillance cameras, erection of security barriers, and closing of approach roads all could be enacted, given sufficient time. In addition to this, security personnel can be placed on high alert and their presence increased. A visible police presence might disrupt the terrorists' plans, causing them to miscarry or abandon the operation. In this regard it is worth mentioning that US embassies overseas work closely with local security services to enhance their physical protection and warn US citizens and businesses to enhance their security posture.

Recovery from terrorist attacks, especially from a chemical, biological, radiological, or nuclear (CBRN) attack, would benefit enormously if governments have timely warning which identifies the likely means the terrorists will use. Armed with this information, specialized responders can be alerted, medical facilities, decontamination plans and equipment prepared, and continuation of vital services and communications assured. The 2001 anthrax attacks in the US in the aftermath of 9/11 are instructive examples. Persons contaminated by some forms of anthrax do not die immediately, nor are most of them likely to die if treated with antibiotics. But, if they are brought to hospitals or allowed to leave the scene and present themselves to hospitals without being decontaminated first, they can, in some cases, spread the spores unknowingly in the ambulances, taxis, or private cars which brought them in. Not only does this risk spreading the anthrax over a far wider area, it also results in the shutdown of treatment by hospitals while they are decontaminated, thereby causing a cascade effect with major consequences for public health.

DOI: 10.19165/2020.6.0120

Warning of this nature should also enable governments to identify experts on the type of the attack, particularly if it is CBRN, and have them available to give accurate assessments to the public.[11] Failure to do so, risks leaving assessments to the media which inevitably will use advocates of the most alarmist interpretation. The author experienced this after the Oklahoma City bombing of the Alfred P. Murrah Federal Building in Oklahoma City on 19 April 1995. On the day of the attack, while teaching at Yale, I received a telephone call from CNN which wanted to know in my opinion which *foreign* terrorist organization or country could be responsible. When this author explained that, given the nature of the target, the location of the attack, and the fact that it occurred on the anniversary of the ending of the Waco siege in Texas, it was most likely an act of domestic terrorism, CNN immediately lost interest.

Public warnings present a special case. Besides possibly inducing terrorists to abandon their plan because it is no longer secret, the main purposes of public warnings are to increase public vigilance and motivation to take protective measures. Public involvement in reporting suspicious behavior or suspicious packages which have been left unattended can bring terrorists and their activities to the attention of the police as under the "see something, say something" initiative.

Avoiding crowded areas at potential target sites is another security precaution the public can be advised to adopt. An example of this behavior is to spend as little time in airport reception areas as possible by checking-in and proceeding through security as quickly as possible. Because these measures require behavioral modification, essentially the public must be induced into adopting them by alerting it to an existing threat. Consequently, with public warning there is a fine balance between releasing enough information to motivate but not enough to cause panic or unnecessary financial loss to businesses. A second problem with threat warnings as a motivator is that their impact lessens with time and is undermined by government reassurances that the situation is under control - reassurances which the government feels it must make in order to retain public confidence. Ironically, these reassurances can, in part, be the result of crisis management and response measures initiated by the warnings. This means that there is an inbuilt tension between the alerting and the reassurance aspects of warning.

Dissemination

Mechanisms for dissemination of warning messages are as varied as the agencies producing them. Generally, they can be grouped by their timeframe and specificity. As examples, I will use those which were in use by the Interagency Intelligence Committee's (IICT) Community Counterterrorism Board (CCB) on behalf of the IC before and after 9/11.[12]

Assessments were equivalent to National Intelligence Council (NIC) memoranda.[13] Their purpose was to provide long-range general analysis of underlying trends, terrorist groups, and to make complex subjects comprehensible, but not simple. When former CIA Deputy Director

[11] Pluchinsky, Dennis A. Anti-American Terrorism: From Eisenhower to Trump, London: World Scientific Publishing Europe, 2020, vol. 1, p. 411.
In 1978, when he reorganized the Working Group on Terrorism (WGT), its new chairman included Public Information as one of its seven standing committees. Its role was to review media guidelines and prepare policymakers to deal with the media during terrorist incidents. -

[12] These Assessments, Advisories, and Alerts were drafted by member agencies of the IC, approved by it, and issued in its name. See the following section for details.

[13] DCI Counterterrorist Center booklet, June 2002.

DOI: 10.19165/2020.6.0120

of Operations Jim Pavitt candidly admitted that while the CIA foresaw the threat Al-Qaeda represented but was unable to predict the exact type and location of its attacks, he spoke to the essence of the distinction between assessments and other forms of warning.[14] Assessments are essential to understanding the nature of terrorist groups and the threats they represent. Some terrorists have limited goals, use discrete and limited violence, and are amenable to negotiations: groups such as the IRA or the Basque nationalist ETA. On the other extreme, some have almost unlimited or apocalyptic goals; they seek mass casualties and are not willing to negotiate: groups such as Al-Qaeda or Aum Shinrikyo, later known as Aleph. Knowing the terrorists' character is of great assistance to police, crisis managers, and crisis responders by allowing them to prepare for the type of operations they are most likely to face. Such assessments are not the sole prerogative of intelligence analysts; strategic warning is the area which is least dependent upon secret intelligence. For this reason, academic and other expert opinions, especially from private organizations (such as the Rand Corp., which for decades has assisted the US government), might be of greater value.

Advisories are much more focused on significant issues and limited in time-frame. An example would be travel advisories such as those issued by the Department of State for US citizens to avoid travel to Lebanon during the 1980s. This advice was usually based upon a rise in anti-US sentiments among some sectors of society, deterioration in the security situation, a political crisis, or intelligence that the terrorist group might be planning to target Westerners.

Alerts are warnings of specific, imminent threats. In the example above, alerts would be a proper response when intelligence indicated that the Lebanese militant group Hezbollah had specific plans to kidnap US citizens. Similarly, in 2011, Russian authorities were given a specific warning of an impending attack on Moscow's Domodedovo Airport. The alert provided authorities with the exact location in the airport, the customs area at arrivals. At the time, Russian security forces were searching for three Chechen suspects. Despite the fact that Russian intelligence services had an excellent idea of who was behind the planned attack and knew their history of causing mass casualties. All that was not known was the timing, but airport authorities knew enough to secure the area, transfer pick-ups away from the airport building, increase police surveillance, and warn the public. Instead, they did nothing and on 24 January 2011 a terrorist bomb killed 37 and injured 183 people.[15] This was a counterintelligence failure not of warning, but of the lack of response to it.

Problems with Warning

There are certain inherent paradoxes in the nature of warning which impact on their ability to perform their mission.

Intelligence Agencies Own the "Alarm Bell" but not the "All-Clear Whistle"

Warnings are generally issued as the result of positive intelligence or analysis about a threat. But seldom is there positive intelligence or analysis that the threat has gone away – such as the neutralization of the terrorists through killing or capture. Consequently, analysts conclude that

[14] Pavitt, James, speech at Duke University Law School Conference, 11 April 2002. Available at:cia.gov/news-information/speeches/testimony.
[15] Gardham, Duncan and Damien McElroy, 'Moscow airport bombing: Russians were warned of imminent attack', *Daily Telegraph*, 25 January 2011. Available at:

DOI: 10.19165/2020.6.0120

just because a threat did not materialize today it will not materialize tomorrow or the day after. That leaves responsibility for staying on alert with the policymaker, who must consider the cost of an alert against the risk of prematurely ending it. An example of this lesson was the 7 July 2005 series of terrorist bombings in London, which killed 52 civilians and injured more than 700 others. The US National Security Agency (NSA) intercepted messages linked to Mohammad Sidique Khan, one of the principal members of the terrorist cell, revealing that he was in contact with Al-Qaeda trained militants in the US. This intelligence was passed to UK intelligence agencies. But US intelligence concluded at the time that nothing in his file indicated he was planning to do something in the UK.[16]

During the summer prior to the attacks, the UK lowered its threat level, encouraging the Metropolitan Police to make officers available for the G-20 summit meeting in Gleneagles, Scotland. Those officers were not available in London when the terrorists struck. It is unlikely that the additional officers would have made any difference, but the timing undermined public confidence.[17]

Warning is a Consensus Position

Warning is the product of bureaucracy, a process in which more persons than just the analyst are involved. Under the UK system, which is characterized by strong central control, intelligence agencies do not make intelligence assessments at all. Instead, they are produced centrally by Cabinet Office assessments staff which strives for consensus. In contrast, the system in the US is more adversarial, reflecting a weaker center. In my day, just after 9/11, although warning products (Assessments, Advisories, and Alerts) were issued under my authority, I first had to task one of the intelligence agencies constituting the IC to draft it, which, of course, involved the analyst's supervisor approving the finished product, usually after peer review in that agency. Then I needed to submit it to the Warn 5 (Warning 5: CIA, DIA – Defense Intelligence Agency, NSA, FBI, and INR – the Department of State's Bureau of Intelligence and Research) together with any other agencies with expertise, for their approval. Dissent, should it occur, was recorded in "footnotes" reflecting differing conclusions. The salient advantage of both systems is their element of peer review, which reduces the element of bias on the part of the analyst. Such analytical problems are often the result of cognitive dissonance when analysts are overloaded with too much conflicting and inconclusive information. Under these conditions, analysts are predisposed to "cherry-pick" only those points that support their preconceptions while dismissing those in conflict with them. This is because one generally requires more information to revise prior conclusions than to confirm them.

There is also the risk of bias, on the part of the agencies themselves which can result in pressure on analysts when warnings or assessments conflict with policy initiatives. During the Iran/Contra Affair, the CIA attempted to use an assessment concerning the American hostages held in Lebanon by Hezbollah to justify the administration's secret policy of selling arms to Iran, which was against the proclaimed policy of the Reagan administration not to make concessions to terrorists. In the end the CIA's efforts failed to sway DIA and INR analysts and

16 Intelligence and Security Committee, Report into the London Terrorist Attacks on 7 July 2007, Ref: ISBN 0101678525, 21 August 2013, Crown Copyright. Available at: Report into the London Terrorist Attacks on 7 July 2005.
Ref: ISBN 0101678525, Cm. 6785PDF, 661KB, 52 pages
[17]Ibid.

DOI: 10.19165/2020.6.0120

the resulting Top Secret assessment concluded that "hostages were neither seized nor released without approval from Tehran."[18]

According to some commentators, the most nearly correct judgements in crisis situations often have been reached by a minority of individuals; when there are disagreements then, the inevitable question is whom to believe – the majority opinion or dissenting opinion of one agency or even one analyst.[19] One of the most famous examples of this was the 2002 assessment that Iraq did have a nuclear program; INR dissented and the subsequent invasion and occupation of Iraq proved it right.[20]

Warning is not a Commodity

Warning is intangible, a hypothesis based upon probability. It is also a transaction between two parties; someone must give it and someone must receive, accept, and understand it. Policymakers often have other sources of information or can be skeptical of intelligence in general. After the Japanese attack on Pearl Harbor, one naval officer observed that, "Possibilities, capabilities and intentions become academic when a does not accept the credibility of his own estimates."[21] In other words, I'll believe it when I see it, but I'll only see it when I believe it. All too often, however, policymakers are disposed to reject warnings not because they are uncomfortable with uncertainty but because it conflicts with their pre-existing views or is critical of their policy's effectiveness. Michael Hayden, former director of NSA and CIA, observed President Trump doing this when he "rejected a fact-based intel assessment because it was inconsistent with a preexisting world view or because it was politically inconvenient …"[22] The ideal was described by former Secretary of State, Colin Powell, when he told INR: "I hold you accountable for the facts, but not for your judgements even if later proven wrong."[23] Regardless of the intelligence, Colin Powell knew that the decision was his and his alone.

"The Drunk and the Lamppost"

An old joke in intelligence circles has it that just like the drunk leaning against a lamppost after a bender, policymakers want intelligence more for support than enlightenment. Few leaders, have had direct experience with intelligence agencies as George H.W. Bush as former head of the CIA and Vladimir Putin as former head of FSB had. For all too many of the remainder their familiarity and expectations often came from a Scottish actor introducing himself on screen as "Bond, James Bond." Much as Bond movies are valued as entertainment, they leave policymakers with an inflated view of what intelligence can do for them. They often read intelligence briefs selectively, looking for confirmation of their beliefs rather than seeing a potentially valuable critique of them. Worse, they may press to see the raw intelligence which underlay the assessment, although they are untutored in evaluating it. It was for this reason that

[18] Martin and, Walcott 1988 Best Laid Plans, p. 360.
[19] Grabo, Cynthia M., *Anticipating Surprise*, National Intelligence Press, 2002.
[20] Efron, Sonni and Greg Miller, Intelligence Veteran Faults Iraqi Arms Data, *Los Angeles Times*, 29 October 2003.
[21] Prange, Gordon, *At Dawn We Slept*, New York: McGraw-Hill, 1981, p. 763.
[22] Hayden, Michael, Gen. Michael Hayden on Perils to Intelligence in the Cyber Age. *Real Clear Politics*, 21 May 2018; Available at: realclearpolitics/video/2018/05/21/full_video_gen_michael_hayden_on_perils_to_intelligence_ in_the_cyber_age.
[23] Instructions to INR's Director.

DOI: 10.19165/2020.6.0120

former Deputy Secretary of State Strobe Talbot instructed INR never to give raw intelligence to senior people.[24]

This is especially true for warning, because it imposes the need for a response on the policymaker, whether positive (acting) or negative (not acting). Warning's key component is threat, which is the combination of the terrorists' intentions and capabilities. In this regard, it is worth mentioning that threat and risk are not the same thing; whereas risk also considers society's vulnerabilities and the countermeasures taken to protect these, warning's role is to help focus countermeasures on those areas most likely to be attacked.

This raises the question: what happens when policymakers feel they cannot afford to take adequate precautions because these may be too expensive or politically unacceptable? One option is to ignore the threat and by default accept responsibility for the heightened risk that results. Another is to pressure warning analysts to reduce their estimate of the threat. An example of the former was related to the author by Nicholas Pratt, director of the Program on Terrorist Strategic Studies at the George C. Marshall European Center for Strategic Studies, about an analysis done for the Bavarian police in preparation for the 1972 Munich Olympic Games, which foresaw an attack by Palestinian terrorists on Israeli athletes and was so prescient that it could have served as a commentary after the event. The scenario was one of 27 prepared by the contractor and it was ignored, possibly because the police found that it conflicted with showcasing the new Germany through a friendly and unarmed police presence.

Another example that is worth mentioning, is the suicide attack on the US Marine barracks on 23 October 1983 in Beirut. The attack was the consequence of the Reagan administration ignoring mounting evidence that the Marines' presence in Lebanon as peacekeepers had been steadily undermined by US actions, such as the bombardment of Lebanese Hezbollah positions by US warships.[25]

In a reverse scenario, the 9/11 Commission, in faulting the failure of the IC to consider aircraft as a suicide weapon instead of as a vehicle for hostage taking, called for "institutionalizing imagination."[26] Wise after the fact, it selected from the spectrum of intelligence available only those items which indicated the former use, while ignoring the far stronger indicators for the latter. Unlimited imagination, however, is no substitute for analysis in the warning process, especially if the potential threat is unlimited such as when CBRN is involved. In November 2001, when Vice-President Cheney was briefed that Pakistan might be assisting Al-Qaeda in making a nuclear weapon, he proclaimed that "if there's a 1% chance that Pakistani scientists are helping Al-Qaeda build or develop a nuclear weapon, we have to treat it as a certainty, in terms of our response. … It's not about our analysis or finding a preponderance of evidence. It's about our response."[27] This reasoning undermines risk-based counterterrorism strategies, which free governments from having to concentrate their limited resources on such worst-case scenarios. It does this by converting hypothetical worst-case dangers into actual threats with enormous cost implications for foreign policy, national security as well as homeland security.

[24] One reason for this caution was that many times 'intelligence' was manufactured by industrious informants because the US was paying for it. In Lebanon it was a cottage industry and so prolific that it gave rise to the term 'rumint' referring to rumor passing for intelligence.
[25] Martin and Walcott 1988, pp. 125-160. The Marines on duty were carrying unloaded weapons and had orders only to fire if fired upon.
[26] *The 9/11 Commission Report*, p. 344 ff.
[27] Suskind, Ron, The One Percent Doctrine, transcript *PBS NewsHour*, 4 July 2006. See also: Suskind, Ron, *The One Percent Doctrine*, New York: Simon and Schuster, 2006.

DOI: 10.19165/2020.6.0120

Intelligence can never be relied upon to get every threat scenario right but, if nearly all hypothetical threats were taken seriously, there would be no need for analysis. Ultimately, such a position would be self-defeating because the flood of warnings for unfounded hypothetical threats would soon obscure those for valid ones.

Even so, analysts must never consider the costs to government or society of issuing warnings as that would politicize analysis. The role of the analyst is to estimate threats; calculating the cost of countermeasures in response is the policymaker's role.[28] Likewise analysts must resist pressure from policymakers to inflate the threat level, either for political or budgetary gain.[29] This separation of role is made much more difficult when the calculation of risk comes from analysts who work in the same organization as the policymakers who are responsible for implementing countermeasures against it.

Structuring Intelligence and the Evolution of Warning

Sherman Kent, who for 20 years directed the CIA's Office of National Estimates, argued that intelligence is organization: "the staff, support, and controls needed to produce the actionable special intelligence that is vital to support the nation's security."[30] Intelligence-derived warnings of terrorist operations or plans are an important part of that special intelligence.

Kent means that good intelligence does not just happen, it is the product of processes inseparable from the bureaucracy that produces it. Intelligence, like some giant super tanker, cannot change direction immediately. Bureaucratic structures take time to evolve, analysts skilled for one field cannot immediately, if ever, reorient themselves for another, and hard-ware designed for one purpose cannot always or easily be redeployed against another. Reconnaissance satellites, for example, cost over a billion dollars and take decades to design and deploy. Since they are in essence in free-fall, they cannot be redirected significantly once in orbit.

Organizational Development and Effectiveness prior to 9/11

The official 9/11 Commission Report begins with a general indictment of the US government, including the IC:

> "We learned that the institutions charged with protecting our borders, civil aviation, and national security did not understand how grave this threat could be, and did not adjust their policies, plans, and practices to deter or defeat it. We learned of fault lines within our government – between foreign and domestic intelligence, and between and within agencies. We learned of the pervasive problems of managing

[28] I am indebted to the former CTC's Deputy Director for Analysis for these insights. They were made in conversation with the Deputy Director of the IICT/CCB on 28 February 2002.
[29] As occurred during the Reagan administration, when it sought to revise statistics on international terrorist incidents to include threats. The effect of this change would have been to double the annual number of incidents. The possible motivation for this change was to justify a tougher foreign policy. See: Pluchinsky 2020, p. lxxxii.
[30] Kent, Sherman, *Intelligence for America's World Policy*, Princeton: Princeton Legacy Library, 2015. For the role Sherman Kent played in the development of CIA's analytic capabilities, see Davis, Jack, 'Sherman Kent and the Profession of Intelligence Analysts,' *The Sherman Kent Center for Intelligence Analysis Occasional Papers*, Volume 1, No 5, 2002.

DOI: 10.19165/2020.6.0120

> and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers."[31]

Although there is much truth in this assessment, it fails to reflect the considerable efforts undertaken by the US government to adjust its structure and policies to newly emerging and ever-evolving terrorist threats. By tracing this evolution, it is possible to see that the success of the 9/11 attacks was, far from being a sweeping example of government stasis, an operational failure in a dynamic environment.

Modern urban terrorism first appeared following the death of Che Guevara in 1967 with the rise of groups such as the Uruguayan Tupamaros, the Brazilian National Liberation Alliance, and the Argentine People's Liberation Army. Other groups soon arose around the world: the Weather Underground in the US, in Japan the Japanese Red Army, in Germany the Red Army Faction, in Italy the Red Brigades, in the UK the Provisional Wing of the Irish Republican Army and the Protestant Ulster Defense Force, and in Spain the Basque Nation and Liberty (ETA). Israel's victory in the 1967 Six-Day War led the Palestine Liberation Organization (PLO) to turn to terrorism and spawned a series of other Palestinian terrorist groups, often supported and at times directed by Syria, Libya, or Iraq. The simultaneous hijacking of four civilian airliners in 1970 by the Popular Front for the Liberation of Palestine (PFLP) is regarded as the start of the modern era of terrorist "spectaculars." Iran only began its rise to become the preeminent terrorist state-sponsor a decade later when in 1982 Iran helped to found Hezbollah among the southern Lebanon's Shia population.

Initially, the US government could not see the forest for the trees. Guerrilla war was familiar, but with terrorism there appeared to be no discernible pattern as groups acted in response to their own agendas, capabilities, target vulnerabilities, and the existing political environment. Viewed by Washington as largely a police matter, counterterrorism policy was left to the Department of State's geographic bureaus on the assumption that terrorism was nothing more than a manifestation of local problems.[32] The CIA took a similar approach. Responding to a Department of State request for information about terrorists, the CIA noted: "the Agency deals with the problem of terrorism on a regional geographic basis by analysts trained in covering a wide range of activities in the countries they specialize on."[33]

One pattern soon emerged that could not be delegated. the escalation of violence, particularly amongst Middle-Eastern groups which were in loose cooperation and competition with each other. In order to retain media attention and to continue to instill fear in the public, terrorists began to make their attacks larger and more violent; hijacking of empty planes soon escalated into taking passengers hostage and then into the murder of one or more of them. Similarly, attacks, such as bombings, escalated into multiple simultaneous attacks. Likewise, suicide attacks initiated by the Popular Front for the Liberation of Palestine (PFLP) were soon copied by other groups as demonstrations of ultimate commitment by their members.

In response to the growing number and severity of incidents, particularly with the PLO's Black September Organization's attack at the Munich Olympics in 1972, President Nixon established a cabinet-level committee chaired by the Secretary of State to combat terrorism. This committee supervised an Interagency Working Group (IWG) consisting of over 30 agencies.

[31] *The 9/11 Commission Report*, p. xvi.
[32] Duncan, Kenneth A., 'Terrorism'; in: Jentleson, Bruce W. and Paterson, Thomas G., *Encyclopedia of U.S. Foreign Relations*, New York: Oxford University Press, 1997, vol., 4 p. 186.
[33] Pluchinsky 2020, p. 309.

DOI: 10.19165/2020.6.0120

At the end of the decade, the Department of State created an Office for Combatting Terrorism to coordinate counterterrorism foreign policy.[34]

On 15 September 1972 CIA began publishing a "Weekly Situation Report on International Terrorism" (WSRIT). Distributed to senior policymakers, the WSRIT listed terrorist threats reported by intelligence and reviewed past terrorist operations for clues to future activities making it an early form of warning threat assessment.[35] The first dedicated threat assessment unit, better known as the Threat Analysis Group (TAG) was created by the Department of State's Office of Security (SY – the forerunner of the Bureau of Diplomatic Security or DS) in 1976. he TAG, was "unique in that it had legitimate analytical and threat assessment responsibilities to monitor terrorism at home and abroad."[36]

President Carter transferred responsibility for counterterrorism from the Cabinet to the National Security Council and, following a 1977 review of US policy procedures, he established the "lead agency" concept for managing terrorist incidents. Under this system agency roles were clearly delineated with responsibility for coordinating response to incidents abroad vested with the Department of State, response to domestic incidents with the Department of Justice (FBI), and response to incidents aboard aircraft with the Federal Aviation Administration (FAA). However, there still was no designation of responsibility for warning. apart from the TAG's role in the protection of US diplomats abroad and foreign dignitaries in the US. A 1982 IC assessment on the role intelligence plays in the fight against terrorism, during the Carter administration noted that there was "continued focusing of policymaker attention on the crisis management and foreign policy aspects of the terrorism problem almost to the exclusion of consideration of the establishment and maintenance of a credible threat assessment capability."[37] This worked to the detriment of warning.

The pace of change quickened during the Reagan administration, which was largely concerned with state-sponsored terrorism. State-sponsors regarded terrorism as a policy tool used to send messages or to impose costs on other states for "unfriendly" actions. Seen from the Cold War perspective, as a form of statecraft, proxy actions were for this reason more easily understood. One of the administration's great concerns was Soviet assistance to the PLO, including the training, funding, and equipping of its fighters, as well as its Eastern Bloc's provision of safehouses for them and of transit for terrorist teams. Poland and East Germany even allowed the Abul Nidal Organization (at one time considered to be the most dangerous terrorist group in the world) to operate businesses openly.[38] But in dealing with Middle-Eastern state-sponsors, the administration lurched from military attacks (e.g. on Libya for the La Belle Disco bombing in Berlin which killed two American servicemen), to covert collaboration (e.g. during the "Iran/Contra affair" the US sold weapons to Iran in the hope of obtaining the release of US hostages and circumventing Congressional scrutiny of its illegal funding of the Nicaraguan Contras).[39]

[34] Duncan, op.cit.,p. 187. Reflecting its growing importance, in 1979 its director, Anthony Quainton, was appointed to the rank of Ambassador while representing the US in international fora. L. Paul (Jerry) Bremer was made the first Ambassador-at-Large for Counterterrorism in 1987 in order to raise further the office's profile, but it was only in 2012 that the Office was elevated to Bureau status.
[35] Pluchinsky 2020, p. 167.
[36] Ibid., p. 314.
[37] Ibid., p. 416.
[38] Duncan, p. 188.
[39] Martin and Walcott 1988, pp. 323 - 366.

DOI: 10.19165/2020.6.0120

In 1982, as a result of lessons learned from the kidnapping and rescue of US Brigadier General James Dozier in Italy, President Reagan established the Interagency Intelligence Committee on Terrorism (IICT) and served as its first chairman. In April that year, he issued a formal National Security Decision Directive (NSDD 30) to charter the IICT under the chairmanship of the Director of Central Intelligence (DCI).

The IICT was the primary forum for coordinating IC counterterrorism activities and for issuing warning products on behalf of the IC. Through its TIERS subcommittee, it produced the IC's ranking of terrorist collection priorities which informed the allocation of resources. Its other functions were reflected in its permanent subcommittees: Warning, Nuclear, Biological, and Chemical Threat, Technical Threat and Countermeasures, and Analytic Training. Connectivity within the IC was an early and continuing responsibility through its management of an electronic community of interest - CT-Link. The IICT was the first recognition, in bureaucratic terms at least, of the importance of warning.

The single greatest impetus for enhancement of US counterterrorism efforts during this decade came from the Vice-President's Task Force on Terrorism. It led the President to reaffirm the role of the IICT with NSDD 207 in January 1986 and to transfer its direction to the National Intelligence Council (NIC) under the National Intelligence Officer for Counterterrorism (NIO/CT).

Another recommendation of the Vice-President's Task Force led to the establishment of the CIA's Counterterrorism Center (CTC).This occurred in 1986 in order to centralize resources engaged in counterterrorism. The CTC was a fusion center, bringing elements of CIA's Directorate of Operations (DO) and Directorate of Intelligence (DI) together with representatives of the FBI, NSA, the Department of Defense (DoD), and other agencies (reaching a total of 30 by 2001). To further concentrate counterterrorism efforts and eliminate possible confusion of roles and responsibilities between CIA and the NIC, the NIO/CT was abolished and IICT transferred to the CTC, effective 1 November 1989. The CTC director then created a Community Counterterrorism Board (CCB) under the Chairman of the IICT to act as its executive.

The CTC was directed to pre-empt, disrupt, and defeat terrorists.[40] Although it reported to the Director of CIA, the majority of CTC managers came from the DO and looked to the Director of Operations for guidance.[41] Since warning did not feature among CTC's primary objectives, however, the IICT/CCB was tangential to the CTC's perceived role. Consequently, an inspection of CTC in 1994 faulted its capacity to provide warning of terrorist attacks.[42]

By these measures, the IC now had a centralized organization (CTC) to conduct the fight against terrorists overseas. Because the IC was not allowed to operate inside the US or to collect intelligence on US citizens, it was not responsible for combatting or warning about domestic terrorism, a role that was reserved to the FBI and the Department of Justice. As 9/11 demonstrated, this was a point of weakness and potential disconnection.

In 1996, the CIA created the Bin Laden Issue Station (nicknamed Alex Station). Under the authority of the CTC, Alex Station was located in the Washington area and was the first virtual

[40] DCI Counterterrorism Center Booklet, p. 7. Reflecting its role to go after terrorists, the CTC was named the Counterterrorist Center rather than the Counterterrorism Center.
[41] *The 9/11 Commission Report*, p. 92.
[42] Ibid., p. 92.

DOI: 10.19165/2020.6.0120

station and the first dedicated to a single issue. Its composition made it a miniature of CTC. Neither the CTC nor Alex Station were perfect; conflicts such as that between CIA, FBI, and DIA persisted.

Merging intelligence and law enforcement was still difficult because of their differing missions, legal authorities, capabilities, and bureaucratic cultures.[43] For Intelligence, as noted, "truth" is unobtainable and assessment of probability is often based upon sources of uncertain reliability and deductions of analysts who never have all the information they need. Law enforcement is concerned with amassing evidence to demonstrate truth in a court of law. Intelligence for law enforcement constitutes "tips" and analysis, as performed by Intelligence, was until recently an alien concept.

The distinction between an Intelligence and Law Enforcement case can be illustrated by the suicide bomb attack on the USS Cole in Aden's harbor in Yemen on 12 October 2000. In spite of the IC's high degree of certainty, its judgement about the responsibility for the attack (which killed 17 US sailors and wounded 39 others) was described as "preliminary" so as not to lead law enforcement to commit to this finding before its own investigations were complete, which could have led to accusations that the administration was acting without conclusive proof.[44]. While they could do nothing about this fundamental difference in concepts of "proof," centers, like the CTC, encouraged sharing of information by providing a secure, collegial environment and aided the development of mutual trust, for we begin by trusting individuals and only later by trusting their institutions.

In many ways the FBI recognized the rise of terrorism, but was unable to respond adequately to it. As far back as 1980, it had established its first Joint Terrorism Task Force (JTTF) with the New York Police Department. Located in the FBI's New York Field Office, it was intended to assist New York Police cope with domestic terrorism. JTTFs expanded to other cities until there were 34 offices at the time of the 9/11 attacks. While these were the primary vehicles for investigating terrorist activity, most were, according to the 9/11 Commission, not fully staffed and state and local entities often believed they had little to gain from full-time participation.[45] Following the World Trade Center bombing of 26 February 1993, FBI Director Freeh told Congress that "merely solving this type of crime is not enough: it is equally important that the FBI thwart terrorism before such acts can be perpetrated."[46] To do this he created a Counterterrorism Division at FBI headquarters to replicate the CTC and arranged for the exchange of senior FBI and CIA officers. But changing the FBI's traditional focus on organized crime, the key element in its preeminent Criminal Division from which came most of the FBI's leadership, proved elusive. In 1998 the FBI issued a five-year strategic plan which for the first time made national and economic security, including terrorism, its top priority, giving prominence to the new Counterterrorism Division over the Criminal Division.[47] But the FBI lacked the resources to fully implement this plan. One critical problem was the lack of properly trained analysts to process the information gathered by the FBI's field agents. Another was the

[43] Wright, Lawrence, *The Looming Tower*, London: Penguin Random House, 2011, p.274 ff. Alex Coleman, the first FBI agent assigned to Alex Station, was first viewed as a spy by Station Director Michael F. Scheuer. Coleman's mission was to gather evidence with the goal of prosecuting Bin Laden, but the only person truly interested was John O'Neil in the FBI's New York Field Office. (New York had responsibility for bin Ladin together with other Islamist terrorists because the Southern District of New York handled the arrest of the blind Sheikh who was involved in the 1993 World Trade Center bombing. *The 9/11 Commission Report*, p. 72,).
[44] *The 9/11 Commission Report*, year,p. 196.
[45] Ibid., p. 82.
[46] Ibid., p. 76.
[47] Ibid.

DOI: 10.19165/2020.6.0120

lack of trained personnel to put that information into a form that could be disseminated. This task was performed at the CIA by its reports officers and to assist the FBI resolve this bottleneck, CIA made some of its own reports officers available. Lastly the FBI's filing system was a shamble resulting from neglect of its traditional paper files and the failure of a computer system that was supposed to have replaced them. As a result, the 9/11 Commission concluded that prior to 9/11 "the FBI never completed an assessment of the overall terrorist threat to the U.S. homeland."[48] Furthermore, the FBI persisted in withholding written reports about its pending investigations because Federal Law prohibited such disclosure in cases which might go before a Grand Jury.[49]

FBI effectiveness was further undermined by the misapplication of procedures initially intended to regulate sharing of information between the FBI and Department of Justice prosecutors. The situation grew more confused as restrictions on sharing information authorized as intelligence collection by FISA Courts (Foreign Intelligence Surveillance Act) were interpreted as prohibiting sharing with FBI agents working on criminal investigations. This created what became known as "the Wall." Ultimately, the FBI came to believe that no intelligence could ever be shared with the Criminal Division even when no FISA Court authorization was involved. This also prevented intelligence gathered by the CIA and NSA from reaching criminal investigators.[50]

Overseas Initiatives

US interests, citizens, and facilities abroad had always been favored targets for terrorists; by 1980 approximately one-third of all terrorist attacks were aimed directly at US personnel or institutions around the world. In response, the Department of State undertook a multimillion-dollar security enhancement program to improve physical security at its US embassies and consulates and established the Bureau of Diplomatic Security to oversee security measures in US foreign missions and protect foreign diplomats at the UN.

Success in reducing terrorist attacks against diplomatic targets came at a price; as "official America" became more difficult to attack, terrorists compensated by turning their attention to "corporate America."[51] In order to discharge both its moral and legal responsibility towards Americans overseas, the Department of State created the Overseas Security Advisory Council (OSAC) to coordinate security and instituted Travel Advisories to provide guidance and warnings to the general public.[52]

On 21 December 1988, PAN AM flight 103 was blown up by a terrorist bomb over Lockerbie, Scotland, killing all 270 on board, including 189 Americans. An investigation by the President's Commission on Aviation Security and Terrorism found that on 5 December 1988 the US embassy in Helsinki had received a threat that within two weeks a bomb would be placed on a PAN AM flight from Frankfurt to the US. The Commission further determined that this threat had been distributed selectively by the FAA and the Department of State, leading to

[48] Ibid., p .77.
[49] Ibid., p. 180.
[50] Ibid., p. 79. *The 9/11 Commission Report* also cites reviews conducted in 1999, 2000, and 2001 that concluded information sharing was not occurring as a result.
[51] Pluchinsky. According to Pluchinsky, citing U.S. Department of State figures, by 1985 the number of attacks on business-related targets exceeded those on overseas US diplomatic and military facilities combined.
[52] Duncan, p. 190.

DOI: 10.19165/2020.6.0120

the accusation of a double standard by warning government employees and not the general public.[53] In 1990, the Congress required, as part of the Aviation Security Improvement Act (Section 109), that the President "develop guidelines for ensuring notification to the public of threats to civil aviation in appropriate cases" - known informally as the "no double standard" policy. In response, the FAA began providing airlines with Aviation Security Bulletins and the Department of State expanded the notification requirement to include non-aviation threats.[54]

Watchlisting terrorists is not always considered a warning function, but it actually plays a key role in warning. Just the knowledge of an attempt to enter the US can be a valuable warning indicator of an impending operation as well as a potential means of frustrating it.

The Department of State's watchlisting program (TIPOFF) was unique because it was the first successful attempt to overcome the barrier between the closed community of secret information and the open world beyond it. Remarkably it was the product of a single INR analyst, who almost unaided conceived, executed, and initially ran the system.[55] TIPOFF, like every watchlisting program, was actually a system involving three key functions: all source data collection, processing and storage in a secure environment combined with a robust capability for finding individuals quickly and accurately, and sharing identifying information on the terrorists beyond the secret world of the IC. TIPOFF's purpose was to aid consular officers overseas and immigration officers at US ports-of-entry (POE) identify suspected terrorists attempting to enter the US. "Hits" were referred to TIPOFF which then coordinated with the IC.

TIPOFF was able to watchlist suspected terrorists on the basis of "reasonable suspicion," such as association with known terrorists. Many of the 9/11 participants, for example, had no previous "terrorist record" but some were known to associate with Al-Qaeda operatives. Since foreigners had no inalienable right to enter the US, this was enough to deny a visa or refuse entry.

TIPOFF also negotiated agreements with Canada and Australia governing the sharing of lookout information and control of secret information, demonstrating the possibility for creating a global lookout system for terrorists.[56]

By 9/11, TIPOFF was the best terrorist watchlist in the US government, but it was not perfect.[57] Reflecting its origins as a border-security support system, it was never intended to be a comprehensive listing of all known terrorists; it was not authorized to hold information on, or to watchlist, US citizens (and alien residents) because they had a right to enter the US and, in

[53] Burton, Fred, The Terrorism Warning Process: A Look behind the Curtain, 16 May 2007.Available at: worldview.stratfor.com, The relevance of a warning from an anonymous informant has been questioned with some analysts saying that it was mere coincidence and the product of a fabricator. Coincidence or not, US government officials were warned and the public was not, which clearly created a double standard.

[54] The 'no double standard' policy is codified under 49 U.S.C. 44905 and the Department of State's Statement of Policy in 7 FAM (Foreign Affairs Manual) 052.1.

[55] For a more comprehensive discussion of watchlisting and its special requirements, see Duncan, Kenneth A., Watchlisting, *Perspectives on Terrorism*, Vol. 10, Issue 5, 5 October 2016, pp. 104-107.

[56] At the Request of FBI Director Freeh, TIPOFF constructed a parallel system for intelligence officers, nuclear, biological radiological, and chemical proliferators, Russian organized crime and other international crime figures, drug traffickers, alien smugglers, and those engaged in economic espionage. According to TIPOFF figures, by 2004, it had over 10,000 entries. It also inspired a cooperative effort between the CIA and the Department of State to furnish a lookout system for Kenya.

[57] In January 2004, John Arriza, TIPOFF's Director, was praised in Congressional Hearings by the 9/11 Commission for nurturing TIPOFF into the most comprehensive watch list in the U.S. government.

DOI: 10.19165/2020.6.0120

any case, the IC was not authorized to collect or store information on US citizens. Its other weakness reflected its origins. As the work of a single analyst and not an IC initiative, the IC did not fully recognize TIPOFF's importance or sufficiently commit to supporting it. In spite of a Presidential Decision Directive (PDD 62) directing CIA to ensure that names of terrorists were to be disseminated to the Department of State, INS (Immigration and Naturalization Service), and FBI so that the border agencies could place them on watchlists, CIA only urged its personnel to support TIPOFF by submitting data on foreign terrorists and left responsibility with the individual without oversight.[58] As the old adage goes "when everyone is responsible, no one is responsible." This was to have dire repercussions on 9/11.

Counterterrorism and Warning Efforts Prior to 9/11

With the passage of time perhaps we can make a more balanced appraisal of the IC's efforts to meet the emerging threat of international terrorism.

The most obvious question that was asked by the 9/11 Committee: "what was the overall strategy to counter the terrorist threat to the United States from 1985 to the present?" CIA"s response was: first, to take the offensive to disrupt terrorist networks and terrorist activity; second, integration of operational, technical and analytical elements in a single large unit collocating analytical and operational activity; and third, community orchestration by serving as the focal point for IC support on terrorism.[59]

For all its shortcomings, missteps, and ultimate failure to thwart both the attack on the World Trade Center in 1993 and 2001, the US had developed new, and transformed existing, counterterrorism structures to implement its strategy. The definitive form of US counterterrorism efforts prior to 9/11 was determined by President Clinton in 1998 under PDD 62 and 63. Together these presidential decision directives defined the nation's critical infrastructure, considered ways of protecting it, and confirmed responsibility for domestic counterterrorism with the Department of Justice and the FBI and with the Department of State and the CIA for foreign terrorism.[60] It is true that these changes were made retrospectively, usually in response to significant terrorist incidents, such as the kidnapping of General Dozier in Italy and attacks on US facilities abroad. This leads critics to argue that the US was preparing to "fight the last war over again"; but this was inevitable.

Major transformative change, such as the creation of the Department of Homeland Security, was never undertaken on hypothetical justifications, consequently what changes were made were largely internal within the IC and Law Enforcement agencies – creation of the IICT, the Department of States' Office for Combatting Terrorism and Bureau of Diplomatic Security, FBI's Counterterrorism Division, and especially CIA's Counterterrorist Center and Alex Station. Such structural changes are relatively easy to make in comparison to changes in bureaucratic culture. Interagency centers, as noted, were important steps in overcoming long standing rivalries and building mutual cooperation but even so it takes time to change attitudes, more than was available before 9/11.

[58] *The 9/11 Commission Report*, p. 505. According to TIPOFF statistics: out of a total of 46,358 documents, the CIA was the largest contributor with 16,622, the Department of State next with 15,950, NSA third with 5,752, then FBI with 1,270, and DIA with 728. All other sources, including open-sources, contributed 6,028 documents.
[59] Q&As for DCI's Presentation for 9/11 Inquiry, answer to question 33, 16 May 2002. Available at:
[60] Ibid., p. 101.

DOI: 10.19165/2020.6.0120

One key flaw was the lack of sufficient terrorism analysts. After three decades of fighting terrorism, there were only approximately 200 analysists throughout the IC specializing in terrorism, most of them at the CIA. According to its public statement: "prior to September 11 (2001), CIA had about 115 analysts including those assigned to CTC itself, who were working terrorism related issues or applying specialized skills to the overall terrorism problem."[61] Their primary purpose was to support covert operations against terrorist organizations and individual terrorists. With regard to warnings, however, the DCI noted that a 2001 inspection of CTC gave its CCB high marks for being an "honest broker" in facilitating and deconflicting views of the community on threat warnings.

James Pavitt, CIA's Deputy Director of Operations, explained the shortcoming that led to 9/11:

> "We've had a number of significant successes over the years, but the fact remains, and I think it's important that I cite this, that we in the Government of the United States as a whole could not … prevent or precisely predict the devastating tragedy of the September 11 attacks. Why do I say that? The nature of the target - we had very good intelligence of the general structure and strategies of the Al-Qaeda terrorist organization, knew and we warned that Al-Qaeda was planning a major strike … what didn't we know? We never found the tactical intelligence, we never uncovered the specifics that could have stopped those tragic strikes …"[62]

CIA Director Tenet was certainly aware of the threat posed by Osama bin Laden. He testified in an open hearing before the Senate Select Committee on Intelligence (SSCI) in February 2000: "Everything we have learned recently confirms our conviction that (Bin Laden) wants to strike further blows against America," and in February 2001, again before the SSCI, he warned "Bin Laden is capable of planning multiple attacks with little or no warning."[63] Not only was the CIA aware of bin Laden's general intentions, CIA's *President's Daily Brief* of 4 December 1998, noted, "reporting – suggests Bin Laden and his allies are preparing for attacks in the US, including an aircraft hijacking to obtain the release of Shaykh Umar Abd al-Rahman, Ramzi Yousef, and Muhammad Sadiq 'Awda … the same source said … that two members of the operational team had evaded security checks during a recent trial run at an unidentified New York airport. …"[64] This certainly qualified as an advisory, if not an alert. Despite its operational failures (see below), it can be argued that the IC got the overall threat assessment of Bin Laden right and warned of one of his likely tactics. Ten years after 9/11, Dan Byman, a professional member of the 9/11 Commission, reflected that: "the intelligence community repeatedly and consistently provided strategic warning that Al-Qaeda was going to attack. George Tenet testified on this publicly before 9/11, and the record is clear of his trying to warn policymakers in both administrations."[65] By concentrating on Al-Qaeda, the DCI actually took a "minority" position. Academics and the media at the time were more concerned with the terrorist threat posed by Iran, its surrogate, Hezbollah, and the IRA. Considering objectively they probably

[61] Harlow, William, Statement by CIA Spokesman Bill Harlow, Office of Public Affairs, provided to the news media in response to their requests, 19 September 2002. Available at:cia.gov/news-information/press-releases-statements/press-release-archive-2002.
[62] Pavitt, 2002.
[63] Harlow, 2002.
[64] Ibid. p. 254 and *The 9/11 Commission Report* , p. 128. In all there were 40 intelligence articles in the *President's Daily Brief* on bin Laden between 20 January 2001 and 10 September 2001.
[65] Byman, Daniel L., Web Chat: The Tenth Anniversary of 9/11, *The Brookings Institute*. Available at: brookings.edu/blog/up-front/2011/09/07.

DOI: 10.19165/2020.6.0120

had valid reasons for doing so, as in past performance Iran/Hezbollah had been the more effective ones in killing Americans.[66]

In the end it was irrelevant whether Bin Laden intended to hijack planes to exchange their passengers for prisoners in US prisons or to fly them into buildings, the salient points were that such a plan was underway and its operatives appeared able to enter the US. And there was "objective evidence" supporting this assessment. On 19 November 1999, Hamidan al-Shalawi attempted to force his way into the cockpit of America West flight 90. Al-Shalawi and a second Saudi were taken into FBI custody but never charged.[67] He was entered into TIPOFF and when he reapplied to enter the US on 5 August 2001 in Riyadh, his visa was denied. THE FBI now believes al-Shalawi's actions had been a dry run for 9/11.

Combined with CIA warning briefings, this incident could have persuaded the government and airlines to reinforce cockpit doors, place additional air marshals on flights, and enhance airport screening, but it was not declassified until years after 9/11. It was a warning that could, but did not happen. Other, vaguer, warnings were given, however. On 2 July 2001, the FBI's Counterterrorism Division sent a summary of terrorist threats from bin Ladin to federal agencies as well as to state and local law enforcement agencies. This summary did not refer to specific types of attack or recommend specific countermeasures.[68] Possibly in consequence of this failure, the US took no comprehensive steps towards improving airport screening and security on flights.

As for the CIA, its best remaining option was to alert the FBI directly and watchlist known Al-Qaeda members. Unaccountably, the CIA failed to do either, allowing two future hijackers, Nawaf al Hazmi and Khalid al Mihdhar, to enter the US undetected, although CIA knew their nationality, passport numbers, and that they both had been in the US and still possessed US visas. Had the CIA done so, it is quite possible both terrorists would have had their visas cancelled or been arrested on or after entry, possibly causing the plan to abort.[69]

Rather than a failure of the IC's organization or of its underestimating the threat posed by Bin Laden or failing to warn about that threat, 9/11 ultimately was an operational failure accountable in part by the nature of the 9/11 plot itself. For while CIA was responsible for foreign terrorists and FBI for domestic terrorists this plot involved foreign terrorists attacking inside the US - a scenario which unintentionally exploited their division of responsibility.[70] But it also reflected a failure to recognize the importance of watchlisting. When these terrorists sought to return to the US, it was a warning indicator that Al-Qaeda's plan was underway and an opportunity to stop it. Finally, it reflected the abiding reluctance of IC members to share information.[71]

---

[66] While Al-Qaeda and its associates killed fewer than 50 Americans in attacks on the US Embassies in Nairobi and Dar es Salaam (1998) and the USS Cole (2000), Hezbollah was responsible for 281 American lives lost in two attacks on the US Embassy Beirut, one on the US Embassy in Kuwait, the bombing of the US Marine barracks in Beirut, the bombing of the Khobar Towers in Saudi Arabia, and the hijacking of TWA 847. It also was responsible for taking 17 Americans, 15 French, 14 British, 7 Swiss, 7 German, and 27 other hostages during the 1980s in Lebanon.

[67] Kalmbacher, Colin, FBI Evidence Said to Implicate Saudi Arabian Government in 9/11 Attacks, *Law & Crime,* 11 September 2017. Available at: lawandcrime.com.

[68] *The 9/11 Commission Report*, p. 258.

[69] Kalmbacher 2017, p. 355.

[70] *The 9/11 Commission Report*, p.263.

[71] On 9/11 TIPOFF contained 1,914 records on Al Qaeda so the reluctance of the CIA to watchlist these particular terrorists was specific. Stranger still, a CTC analyst in August 2001, while reviewing their files,

DOI: 10.19165/2020.6.0120

Post 9/11 - Bin Laden and Beyond

The attacks of 9/11 were so momentous that they resulted in a paradigm shift both in appreciation of the risk terrorists posed for society and in the size and scale of the response. In light of the damage wrought by bin Laden, this new form of terrorism was known as "catastrophic terrorism." It is characterized by rigid religious views impervious to challenge on moral grounds, greater willingness to die, and greater lethality, with few inhibitions on targeting civilians or using CBRN.[72]

Confronting this post-9/11 reality a much-chastened government and especially IC began to transform themselves. US priorities were defined as: defend the homeland, defeat global terrorist networks, diminish the capacity of new groups to form, and deny terrorists safe havens. Yet these new priorities were in many ways just modifications of existing goals. The real difference lay in the realization of what would be required to achieve them. What was new was the underlying understanding that fighting the new terrorism would have to be a community effort, requiring fusion of intelligence, law enforcement, military and diplomatic responses, together with new partners at the federal, state and local level who were responsible for homeland security, border security, crisis management and crisis response. That entailed fixing responsibility among new and old players, with recognition of the primacy of warning and risk-vulnerability calculations. Successful implementation needed the creation of permanent structures to institutionalize and communicate warning not just within government, be it federal, state, or local, but throughout the entire population.

The first step towards reorientation came in September 2001 with the restructuring of the National Security Council as terrorism was split from infrastructure security.[73] This was followed by the creation of a parallel organization: the Homeland Security Council, first headed by Governor Tom Ridge, who went on to become the first Secretary of the Department of Homeland Security (DHS), when that department was established.
DHS brought together agencies responsible for domestic security: Coast Guard, Transportation Security Administration (TAS), Federal Emergency Management Agency (FEMA), Immigration and Naturalization Service (INS), US Customs, Border Patrol, and Secret Service (which soon may revert to Treasury). Full integration into the IC was critical to the fulfilment of several of its missions, notably to perform vulnerability studies and map threats against vulnerabilities; set national priorities for infrastructure protection; and, most importantly, to issue warnings directly to the American people. Accordingly, it set up a new intelligence unit under an Assistant Secretary for Analysis, which became part of the IC as well as the Warn 5 group (creating the Warn 6), which reviewed all IC warning products. In addition, DHS' Homeland Security Operations Center (HSOC) was made responsible for warning federal, state, and local officials as well as the private sector and the public through its National Terrorism Advisory System (See Public Warning below).

In parallel with the FBI's JTTFs, HSOC is connected to Antiterrorism Task Forces (ATTF), which now can be found in every state and most major cities throughout the US, and with private sector security programs through the American Society for Industrial Security (ASIS).

noticed this omission and sent their names to TIPOFF. Unfortunately for the US, the two already had entered the country. Conversation of the author with the analyst. See also: Ibid., p. 270.

[72] *The 9/11 Commission Report*, pp. 47 - 63.

[73] General John Gordon was made a new Deputy National Security Advisor for Terrorism. Dick Clarke was given Infrastructure Security.

DOI: 10.19165/2020.6.0120

ASIS members received a daily unclassified report from DHS and reported back any suspicious activity.[74]

Warn, and through it, protect America became the watchword. The IC itself was transformed in recognition of the importance of warning. At its apex was a new Director of National Intelligence (DNI). The DNI is supposed to be a central hub for coordinating the IC – a role the DCI, it was thought, could not play because of rivalries between agencies, particularly FBI and DIA with CIA - and would be able to oversee domestic as well as foreign intelligence collection, something the DCI could not do. It was also believed that the head of the IC should not be both one of the advocates and the judge of them all in setting priorities for funding.[75] There are issues, however, particularly with the enhanced risk of politicization as US presidents are not required to appoint individuals with an intelligence background.[76] Such an issue emerged when the new DNI, John Ratcliffe, a Trump loyalist, notified Congress that there would be no further in-person intelligence briefings on foreign interference in the 2020 elections. In their place classified memoranda would be provided, but the change gave rise to accusations that it was intended to stifle Congress' ability to question the DNI about Russian interference.[77]

Reporting directly to the DNI are the NIC and a newly created organization, the National Counterterrorism Center (NCTC), which began operations in December 2004, subsuming the Terrorist Threat Integration Center (TTIC). TTIC itself had been created in June 2003 to close the seam between analysis of foreign and domestic terrorism. Drawing staff from throughout the IC but principally from the CTC, its key function was threat analysis and warning. TTIC took over CTC's responsibilities for maintaining a threat matrix of all known terrorist plots against the US.

Twice daily TTIC conferred with FBI and other agencies via a secure video teleconference at which the matrix was reviewed and actions agreed upon. It drafted Senior Executive Intelligence Bulletins and Executive Memorandums as well as spot commentaries.[78]. TTIC also assimilated the IICT with its warning functions and responsibility for connectivity. After 9/11, CT-Link, which became TTIC On-Line, grew to over 100 member agencies and departments, including representatives of all three branches of government, making it the largest classified community of interest in the US government.

When it solved the problem of warning with new organizations, the IC inadvertently contributed to another: the chronic shortage of trained terrorism analysts. As noted, on 9/11 there were hardly 200 available within the entire Federal Government. Now that warning in the form of TTIC was separated from counterterrorist activities in the CTC, those analysts who had transferred from CTC to TTIC were no longer available to support its operations and vice

[74] Hulnick, Arthur, Indications and Warning for Homeland Security: Seeking a New Paradigm, *International Journal of Intelligence and Counterintelligence*, Vol. 18, No. 4., Winter 2005, p. 5.
[75] *The 9/11 Commission Report*, year p. 411 ff. Creation of the DNI draws the US closer to British practice – where the Joint Intelligence Committee (JIC) traditionally functions under the chairmanship of a representative of the Foreign and Commonwealth Office who does not directly control collection assets.
[76] The first DNI, John Negroponte, was a Senior Foreign Service Officer with extensive experience as an intelligence consumer.
[77] Sanger, David E. and Julian E. Barns, Shift on Election Briefings Could Create an Information Gap for Voters, *New York Times*, 30 August 2020.
[78] See the FBI's A New Era of National Security, 2001-2008 (Available at: fbi.gov/history/brief-history /a-new-era-of-national-security) in which FBI describes its participation on the Matrix and closer cooperation with CIA as part of its response to 9/11.

DOI: 10.19165/2020.6.0120

versa. Creation of the NCTC and intelligence centers and cells in agencies, such as DHS, throughout government further contributed to the already critical shortage of analysts, who were needed more than ever as more intelligence on terrorism began to flood in.[79]

According to its director, the NCTC was the result of the 9/11 Commission's recommendation for a "civilian-led unified joint command for counterterrorism." Pursuant to this role, the NCTC prepared a National Implementation Plan for Counterterrorism (NIP) containing four pillars: (1) protect and defend against terrorists, (2) attack their capacities to operate, (3) work to undermine the spread of violent extremism, and (4) prevent terrorists from utilizing WMD. Established in June 2007, the NCTC's Interagency Task Force (ITF) is charged with ensuring US government counterterrorism activities are "correlated rapidly" in response to changes in the "threat picture and level of risk" and formulates domestic and overseas options for senior policymakers.[80] Interestingly, for an agency created from TTIC, nowhere in the director's summary of its priorities and role did the word "warning" appear. The NCTC does develop and facilitate national, international, and local exercises and shares lessons learned with DHS and FBI - contributing to the pre-emption and mitigation roles of warning, but domestic (public) warning is now vested with DHS. One consequence of this realignment was to place responsibility for domestic warning of terrorist threats and their mitigation and response in one agency, which could lead to conflicts of interest as indicated above.

TIPOFF was a victim of its own success. There was no other program for declassifying and using intelligence to identify terrorists, nor was there another comprehensive database for all-source terrorist intelligence.[81] But the terrorist attacks of 9/11 demonstrated that the threat was ubiquitous and certainly could include US citizens. TIPOFF was transferred to TTIC and now has two successors. The first is the Terrorist Identities Datamart Environment (TIDE) which is a compendium with over 25,000 US citizens among its one million plus entries. The second is the FBI's Terrorist Screening Center's Database and its No-Fly List.[82]
The FBI transformed itself, making terrorism and warning key priorities.[83] This change was reflected structurally by combining its Counterterrorism, Counterintelligence, and Intelligence Divisions into a National Security Branch, officially on 12 September 2002, and by performing triage on its organized crime activities by transferring 900 special agents from crime to terrorism (and hiring hundreds of others) – leaving many of its traditional criminal investigations to be conducted by other law enforcement agencies. Another priority was Domain Management – a program to move beyond chasing criminals to gathering intelligence. An ex-CIA analyst was responsible for the program which has had problems similar to the Wall – fear of uncontrolled domestic spying. This was in spite of passage by Congress of the 'Patriot Act' in 2001, which introduced sweeping changes in how electronic surveillance was to be conducted and how financial transactions were to be accessed, among other areas.[84] The Act's

[79] The 9/11 Commission lists five analytic centers: CTC, TTIC, DIA, DHS, and FBI and questions whether the US government can afford such duplication in efforts. *The 9/11 Commission Report*, p. 401.
[80] Leiter, Michael, Eight Years after 9/11: Confronting the Terrorist Threat to the Homeland, Statement before the Senate Homeland Security and Governmental Affairs Committee, 30 September 2009.
[81] TIPOFF brought over 130,000 names of known or suspected terrorists and the record of over 70,000 'hits' against those names.
[82] Fram, Alan, Why can people on the terrorist watchlist buy guns and other FAQs, *Associated Press,* 14 June 2016.
[83] Pistole, John, Deputy Director FBI, address at the George C. Marshall Center. See also: A New Era of National Security, 2001-2008.
[84]The Patriot Act's official title is 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001'. For provisions of the act see: The Department of Justice, The USA PATRIOT Act: Preserving Life and Liberty. Available at: justice.gov/archive.

DOI: 10.19165/2020.6.0120

intention was to improve sharing of information among law enforcement agencies, regulators, and financial institutions.

The FBI took a leadership role in liaison with state and local police officials. It established secure (classified) connectivity by constructing Sensitive Compartmented Information Facilities (SCIF) within its regional offices' JTTFs. Governors and key officials, as well as state and local police, now were able to access secure intelligence through TTIC On-Line in these SCIFs. Cooperation was a two-way street as locally obtained information could now flow back to Washington, making local authorities both producers as well as consumers of intelligence.

Instituting Effective Public Warning

This arrangement had its drawbacks, however. It was not inclusive enough. Essentially key officials were admitted into the "secret club" but this was not the same thing as public warning. To make public warning effective the IC had to transform its intelligence into information that could be widely/universally disseminated to private citizens. Credit for first undertaking this transformation goes to NSA which began including unclassified attachments, on its TOP SECRET intelligence products. The IICT/CCB broke new ground when it published the first joint FBI/CIA terrorist threat assessment in both a secret and unclassified format.[85] It also organized an open conference on suicide bombers, which resulted in guidelines for security officers on key behaviors and suggested countermeasures.[86]

There were still problems with this solution. It is far easier to share general analysis or conclusions, which by their general nature make it easier to protect sources and methods, than it is to share highly sensitive intelligence about terrorists' specific intentions. Unfortunately, this is in inverse proportion to the utility of the information for homeland security officials. They need to know which specific targets are most at risk so that they can best allocate their always limited resources in an environment containing almost unlimited vulnerabilities.

Public warnings through color-coded warning systems were not the answer. In May 2011, the US gave up its much-maligned color-coded Homeland Security Threat Advisory System. New York and Arizona already had abandoned it and few mourned its passing. Its major flaw was that it was constantly "on." Blue and Green signifying all's quiet were never used because they did not reflect world terrorist levels; red was impossible to sustain because of its effect on the economy; and consequently, it fluctuated between yellow and orange. In the words of Congressman Bennie Thompson: "The old color-coded system taught Americans to be scared, not prepared. Each and every time the threat level was raised, very rarely did the public know the reason, how to proceed, or for how long to be on alert."[87] A warning system that is

For criticisms of the act see: Aclu, Surveillance Under The Usa/Patriot Act. Available at: aclu.org/other/surveillance-under-usapatriot-act.

[85] Intelligence Community/Law Enforcement Community Terrorist Threat Assessment: Current Terrorist Threats to the United States, *Community Counterterrorism Board*, (U) 26 February 2002.

[86] Law Enforcement Sensitive: Suicide/Homicide Attacker Behaviors – And Suggested Countermeasures, *Community Counterterrorism Board*, 6 January 2003.

[87] National Terrorism Advisory System, Wikipedia.org.

DOI: 10.19165/2020.6.0120

constantly blinking danger ultimately desensitizes people to the reality of the threat when it actually occurs.[88]

It was replaced by DHS' National Terrorism Advisory System (NTAS), which only has two elements: Bulletins (old assessments), which communicate general developments or general trends and Alerts, which communicate information about credible threats. There are two types of Alert: Elevated (old advisories) when there is only general information about the timing and target and Imminent (old alerts) if there is information that the threat is credible, specific, and impending. Alerts contain a "sunset provision" that marks their expected expiration date.[89] The new system is designed to provide clear, timely, and above all specific information about the threat.

The reverse is also a problem with warning when there is too much, rather than too little intelligence. These risks drown analysts or customers in terabits of useless data. We do not have enough analysts to wade through all the material being collected by our own intelligence and law enforcement agencies as well as that passed to us from foreign ones, and obtained from world-wide open sources. In managing this shift from "cleared to know" to "need to know," one must be mindful that intelligence sharing must not be sharing everything to everybody. Just as DHS has done with its NTAS, intelligence information must be disseminated according to need: on the grand scale to give the big picture with information about groups, their supporters, funding, recruitment, training, objectives, and capabilities; as well as, on the individual scale, the activities, movements, and connections of individual terrorists. One last point, the interface of intelligence information and regulatory agencies who are responsible for watchlisting and blacklisting individuals or organizations, involves the implicit obligation to establish procedures to vet and review information and to remove the incorrectly or falsely accused quickly.

Conclusion

"*Deye mon, gen mon*" (beyond the mountains, more mountains) is an old Haitian proverb meaning beyond today's problems lie still more problems. This is an apt metaphor for our ongoing involvement with terrorism for, in the words of Australian criminologist Grant Wardlaw, "there is no cure for terrorism, not through massive security measures at home and the projection of military force abroad."[90] This is not a counsel of despair, for just as we cannot eliminate terrorism any more than we can ordinary crime, we still can minimize it, reduce its impact, and anticipate its changing forms.

The IC stems from the traumatic event of 9/11. Between 2001 and 2018, the US spent at least $2.8 trillion USD on counterterrorism, which according to the Stimson Center, is approximately 15 per cent of the US government's discretionary budget. Most was spent in Iraq and Afghanistan, but $979 billion USD went to homeland security, representing about 35 percent of the counterterrorism budget. For that sum the US eliminated Bin LadEn, diminished Al-Qaeda, and assisted in the dismemberment of ISIS. In view of this, it is noteworthy that,

[88] Australia's threat system had been stuck for 13 years at medium until raised in 2015 to high by the Prime Minister. Bergin, Anthony and Claire Murphy, 'Fair Warning: Australia's terrorist advisories', *The Strategist*, Australian Strategic Policy Institute, 16 April 2015.
[89] Homeland Security, NTAS Frequently asked questions. Available at: dhs.gov.
[90] See Wardlaw, Grant, *Political Terrorism: Theory, Tactics, and Countermeasures*, Cambridge: Cambridge University Press, 1982.

DOI: 10.19165/2020.6.0120

during this period, only 100 people were killed on US soil as a result of Islamic terrorism with the result that approximately 100 persons were killed in the US during this period by Islamist terrorists.[91]

Although some terrorist threats have been diminished, we should never forget that terrorism's enduring threat lies not only in the damage it inflicts but also in the psychological impact it has, by promoting panic and overreaction.[92] While traditional groups, remain a threat, terrorism's new frontiers lie, for the moment at least, with independent cells or lone-actors, who in addition to the traditional bomb, bullet, hijacking, and kidnapping may turn to novel forms of attack such as sowing computer viruses or ransom ware, hacking systems, or employing CBRN agents. These actors may be joined by "professional" protestors who target international meetings, such as the G-20, and exploit demonstrations against local grievances in the hope of provoking government over-reaction. Conceivably they could return to the domestic terrorism which plagued the 1970s. And they may be joined by others such as right-wing, Neo-Nazi, and neo-anarchist groups and individuals.

Warning in the form of identifying and calculating the risks posed by these actors and their methods, will require looking beyond the threats themselves at their secondary effects – especially to the environment. It will need to be focused on assisting state and local authorities, especially police and first responders identify these novel threats and guide them on how best to respond to them, as the NCTC is now doing. One thing is certain, the IC and US government must recognize that failure to warn prior to a terrorist attack results not just in physical damage to society but also in diminished confidence in those agencies responsible for protecting citizens, especially when it is later revealed that information was withheld that could have prevented loss of lives. This cost of loss of public confidence generally outweighs the costs of divulging secret intelligence.

Yet, the IC's operation in a domestic context also raises troubling questions because while good relations with local communities are essential, those relations can be undermined by the very surveillance techniques used both in detection and response. Measures such as ethnic, political, and religious profiling, camera surveillance of public spaces, and electronic monitoring based on warning indications rather than probable cause are problematic. Warning inspired prevention measures, such as premature arrest and shooting potential suicide bombers also raise profound human rights concerns.[93] As a UN Report notes: increased scrutiny for potential male suicide bombers who may be disguised as females may make transgender persons, transvestites, and intersex (those in the midst of a sex change process) susceptible to increased harassment and suspicion.[94] This admittedly is an extreme case but inevitably there will be trade-offs between respect for the rights of individuals and organizations (such as mosques) and the protection of society. Where to draw the line is of fundamental importance if we do not wish to sacrifice our way of life in order to protect it.

[91] Donheiser, Julia, The United States Has Spent At Least 2.8 Trillion On Counterterrorism Since 9/11, *The Center for Public Integrity*, 18 May 2018. Available at: publicintegrity.org.; Heeley, Lacy, First Full Accounting of US Counterterrorism Finds US has Spent $2.8 Trillion, *Stimson*, 16 May 2018. Available at: stimson.org.
[92] Duncan, p. 191.
[93] Witness the police shooting of the innocent Jean Charles de Mendez in 2005 two weeks after the 7 July 2005 bombings in London on the mistaken assumption that he was another suicide bomber.
[94] Scheinin, Martin, 'Report on the Protection of Human Rights and fundamental freedoms while countering terrorism', New York: United Nations, 2009.

DOI: 10.19165/2020.6.0120

Throughout this chapter, this author has been guided by Sherman Kent's observation that intelligence is a matter of organization; you get the intelligence and warning you prepare for. This raises similar questions to those asked about the IC prior to 9/11: whether after spending billions on a revamped IC just how fit for purpose is it today in dealing with mini-cells and individual terrorists and whether it is the proper agent to do so?

Terrorists are often funded through petty crime, recruited in prisons, and exhibit behavioural changes noted by their local communities and so domestic collection today is best undertaken by local law enforcement and the FBI.

The IC can best contribute to protecting society by continuing to fight foreign terrorists, first by enhancing the sharing of intelligence through a network of sister fusion centers around the world, second, by continuing to turn intelligence into information that can be shared widely outside as well as inside the US, and finally, by supporting and encouraging watchlisting with foreign partners, as was initiated by TIPOFF with Canada and Australia.

As we plan tomorrow's Intelligence Community, we should not do so on the basis of either the present terrorist threat or the past one, represented by 9/11. Today's new terrorism is not the sole or main threat to domestic or global security and the IC's efforts at collection, analysis, and warning will need reflect this. State-sponsors such as Iran and its primary surrogates, Hezbollah and Iraqi Shia militias, remain active. A new state-sponsor and worse has reemerged with Russia's activities in Ukraine. Failed or failing states, such as Somalia, Libya, Afghanistan, Syria, Venezuela, and Yemen may spawn potential terrorist threats.

While terrorism is important, so too are more traditional global threats: emerging nuclear powers North Korea and Iran, conflicts between nuclear powers such as India and Pakistan, and the rapidly emerging super-power China, to name a few. The relatively new threats of computer hacking and denial of service attacks are escalating dramatically. In 2007, cyber hackers targeted Estonia's parliament, banks, government, and media, giving a foretaste of what future cyber-assaults could do as dependence on cyberspace continues to grow.[95] Russia's attempts to manipulate the US presidential elections in 2016 and 2020, the UK's Brexit and Scottish independence votes, as well as other elections in Europe, reflect the dawn of a new electronic Cold War. Russia, China, and Iran, in particular, are developing robust capabilities in this field. This will be a challenge for the IC and warning because it unites threats from states, international criminal organizations, cyber-terrorists, and individuals and will require new partners and new skills to identify new threats as they evolve and to provide timely guidance in defeating them.

Finally, in recognition of the enduring threat of terrorism, we have seen new agencies emerge, particularly to warn and protect the homeland. Such institutionalization of our counterterrorism efforts serves to fix responsibilities but also massively increases the size of the bureaucratic pyramid. We must be mindful of the over-specialization this can entail. Specialization does not always lead to greater effectiveness; it can also lead to the endless production of reports, bureaucratic empire building, and maintenance of hierarchy. The impact of these tendencies can be debilitating because intelligence analysis and warning depend upon initiative, integrity, and freedom from politicization that are difficult to accommodate in ever growing bureaucracies. A decade ago, Harold Ford, one of CIA's premier analysts, cautioned: "In the

[95] Russia is believed to be responsible for these attacks. According to Sergi Markov of the Russian Duma, his aide was responsible for their coordination. Markov said the aid acted on his own and Russia denies any involvement. See: Coalson, Robert, Behind the Estonia Cyberattacks, *Radio Free Europe*, 6 March 2009.

DOI: 10.19165/2020.6.0120

last analysis, however, improvements will not rest so much on organizational or procedural changes, whatever their nature, as on the caliber, cooperativeness, and integrity of the individual officers who produce intelligence. And even more on the caliber, cooperativeness, and integrity of the individual officers who consume intelligence."[96]

Kenneth A. Duncan is a retired US Senior Foreign Service Officer. On 5 September 2001, he became Chairman of the Interagency Intelligence Committee on Terrorism and its Community Counterterrorism Board. In this capacity he was responsible for providing formal warning of terrorist threats on behalf of the Intelligence Community to the highest levels of the Federal Government and for formulating and levying intelligence collection requirements on the Intelligence Community. Prior to his selection for this post by the Director of Central Intelligence, he was Charge d' Affairs, a.i., at the US Embassy in Haiti. He also served in the Department of State's Bureau of Intelligence and Research (INR) as Director of the Office of Intelligence Coordination and as Deputy Department representative on the National Counterintelligence Policy Board. As such he was Senior Advisor to the Secretary of State for all matters involving counterintelligence and sensitive law enforcement activities. He also served as the analyst for Middle-Eastern terrorism in INR and taught courses on terrorism at Yale University and at the United States Coast Guard Academy. On retirement from the Foreign Service, he became Senior Adjunct Professor of Terrorism at the George C. Marshall European Center for Strategic Studies in Garmisch-Partenkirchen, Germany.

[96] Ford, Harold, *Estimative Intelligence: The Purpose and Problems of National Intelligence Estimating*, Lanham, Md.: University Press of America, 1992.

DOI: 10.19165/2020.6.0120

Bibliography

ACLU, SURVEILLANCE UNDER THE USA/PATRIOT ACT, Available at: aclu.org/other/surveillance-under-usapatriot-act.

BBC, "Yemen parcel bomb 'was 17 minutes from exploding'", 4 November 2010.

Bergin, Anthony and Murphy, Claire, "Fair Warning: Australia's terrorist advisories", *The Strategist*, Australian Strategic Policy Institute, 16 April 2015.

Burton, Fred, "The Terrorism Warning Process: A Look behind (stet) the Curtain." Available at: worldview.stratfor.com, 16 May 1 2007.

Byman, Daniel L., "Web Chat: The Tenth Anniversary of 9/11", The Brookings Institute. Available at: brookings.edu/blog/up-front/2011/09/07.

Coalson, Robert, "Behind the Estonia Cyberattacks", *Radio Free Europe*, 6 March 2009.

Davis, Jack, "Sherman Kent and the Profession of Intelligence Analysts", *The Sherman Kent Center for Intelligence Analysis Occasional Papers*: Volume 1, No 5. 2002.

DCI Counterterrorist Center booklet, June 2002.

Donheiser, Julia, "The United States has spent at least 2.8 trillion on counterterrorism since 9/11," *The Center for Public Integrity*, 18 May 2018. Available at: publicintegrity.org.

Duncan, Kenneth A., "Terrorism"; in: Jentleson, Bruce W. and Paterson, Thomas G., *Encyclopedia of U.S. Foreign Relations*, New York, Oxford University Press, 1997, Vol. 4.

Duncan, Kenneth A., "Watchlisting", *Perspectives on Terrorism*, 5 October 2016, Vol. 10, Issue 5.

FBI, "A New Era of National Security, 2001-2008." Available at: fbi.gov/history/brief-history/a-new-era-of-national-security.

Efron, Sonni and Miller, Greg, "Intelligence Veteran Faults Iraqi Arms Data", *Los Angeles Times*, 29 October 2003.

Ford, Harold, *Estimative Intelligence: The Purpose and Problems of National Intelligence Estimating*, Lanham Md., University Press of America, 1992.

Fram, Alan, "Why can people on the terrorist watchlist buy guns and other FAQs", *Associated Press*, 14 June 1 2016

Gardham, Duncan and McElroy, Damien, "Moscow airport bombing: Russians were warned of imminent attack", *Daily Telegraph*, 25 January 2011.

Government response to the Intelligence and Security Committee report into the London terrorist attacks on 7 July 2005, Ref: ISBN 0101678622, 21 August 2013, Crown Copyright.

Grabo, Cynthia M., *Anticipating Surprise*, National Intelligence Press, 2002.

Harlow, Willian, "Statement by CIA Spokesman Bill Harlow, Office of Public Affairs, provided to news media in response to their requests", 19 September 2002. Available at:cia.gov/news-information/press-releases-statements/press-release-archive-2002.

Hayden, Michael, "Gen. Michael Hayden on Perils to Intelligence in the Cyber Age. Real Clear Politics", 21 May 2018.
Available at: realclearpolitics/video/2018/05/21/full_video_gen_michael_hayden_on_perils_to_intelligence_in_the_cyber_age.

Heeley, Lacy, "First Full Accounting of US Counterterrorism Finds US has Spent $2.8 Trillion", *Stimson*, 16 May 2018. Available at: stimson.org.

Hoffman, Bruce, and Ware, Jacob, "The Challenge of Effective Counterterrorism Intelligence in the 2020s", *Lawfare*, 21 June 2020. Available at: lawfareblog.com.

Homeland Security, NTAS Frequently asked questions. Available at: www.dhs.gov.

DOI: 10.19165/2020.6.0120

Hulnick, Arthur, Indications and Warning for Homeland Security: Seeking a New Paradigm, *International Journal of Intelligence and Counterintelligence*, Winter 2005, Vol. 18, No. 4.

Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2007*, Ref: ISBN 0101678525, 21 August 2013, Crown Copyright.

Kalmbacher, Colin, "FBI Evidence Said to Implicate Saudi Arabian Government in 9/11 Attacks", *Law & Crime*, 11 September 2017. Available at: lawandcrime.com.

Kent, Sherman, *Intelligence for America's World Policy*, Princeton, NJ, Princeton Legacy Library, 2015.

Leiter, Michael, "Eight Years after 9/11: Confronting the Terrorist Threat to the Homeland", Statement before the Senate Homeland Security and Governmental Affairs Committee, 30 September 2009.

Martin, David C. and Walcott, John, *Best Laid Plans*, New York, Harper and Row, 1988.

National Terrorism Advisory System, Wikipedia.org.

Petersen, Michael, "What I Learned in 40 Years of Doing Intelligence Analysis for US Foreign Policymakers" *Studies in Intelligence*, March 2011, Vol 55, No. 1.

Prange, Gordon, *At Dawn We Slept*, New York, McGraw-Hill, 1981.

Pluchinsky, Dennis A., *Anti-American Terrorism: From Eisenhower to Trump*, London, World Scientific Publishing Europe, 2020, vol. 1.

Palombi, Simon, "'Known to Police': Assessing Terrorism Risk", 18 March 2015.Available at: Chathamhouse.org/expert/comment.

Pavitt, James, speech at Duke University Law School Conference, 11 April 2002. Available at: cia.gov/news-information/speeches/testimony.

Q &As for DCI's Presentation for 9/11 Inquiry, answer to question 33, 16 May 2002

Sanger, David E. and Barns, Julian E., "Shift on Election Briefings Could Create an Information Gap for Voters', *New York Times*, 30 August 2020.

Scheinin, Martin, *Report on the Protection of Human Rights and fundamental freedoms while countering terrorism*, New York: United Nations, 2009.

Suskind, Ron, "The One Percent Doctrine", transcript *PBS NewsHour*, 4 July 2006.

Suskind, Ron, *The One Percent Doctrine*, New York, Simon and Schuster, 2006.

The Department of Justice, The USA PATRIOT Act: Preserving Life and Liberty. Available at: justice.gov/archive.

The 9/11 Commission Report. New York, W.W. Norton & Company, 2004.

UK Government Response to the Intelligence and Security Committee's Report into the London Terrorist Attacks on 7 July 2005.

UK Intelligence and Security Committee: *Report into the London Terrorist Attacks on 7 July 2005*.

Wardlaw, Grant, *Political Terrorism: Theory, Tactics, and Countermeasures*, Cambridge, Cambridge University Press, 1982.

Whitehead, Tom and Foster, Peter, "Al-Shabaad calls for attacks on Oxford Street and Westfield centres in new terror threat", *The Telegraph*, 22 February 2015.

Wright, Lawrence, *The Looming Tower*, UK, Penguin Random House: 2007

DOI: 10.19165/2020.6.0120

Further reading

Agrell, Wilhem, "When everything is intelligence – nothing is intelligence," *Sherman Kent Center for Intelligence Analysis, Occasional Papers*: Vol.1, No.4.

CIA Sherman Kent Center for Intelligence Analysis Papers: Practice of Analytic Tradecraft in the Directorate of Intelligence, Transnational Threats, Profession of Intelligence Analysis, Progressive Management, 2013.

Davies, Philip, H.J., "Intelligence Culture and Intelligence Failure in Britain and the United States", *Cambridge Review of International Affairs*, October 2004, pp. 495-520.

Davis, Jack, "Tensions in Analyst-Policy Maker Relations: Opinions, Facts, and Evidence", *Sherman Kent Center for Intelligence Analysis, Occasional Papers:* 2003, Vol. 2, No. 2.

Dulles, Alan, *The Craft of Intelligence*, Guilford, CT., The Lyons Press, 2006.

Durbin, Brent, *The CIA and the Politics of US Intelligence Reform*, Cambridge University Press, 2017.

General Accounting Office (GAO), "Combatting Terrorism, Interagency Framework and Agency Programs to Address the Overseas Threat", May 2003.

Gates, Robert M., "An Opportunity Unfulfilled: The Use and Perception of Intelligence in the White House", *Washington Quarterly*, Winter 1989.

Greenberg, Maurice R., Chairman, "Making Intelligence Smarter: The Future of U.S. Intelligence", *Council on Foreign Relations*, 17 February 2005 Available at: fas.org/irp/cfr.html .

Handel, Michael, "Intelligence and Strategic Surprise", *The Journal of Strategic Studies*, 1984, Vol 7, No.3.

--The Politics of Intelligence, *The Journal of Strategic Studies*, 1987, Vol. 2, No. 4.

Hass, Richard N., "Supporting Us (sic) Foreign Policy in the Post 9/11 World", *Studies in Intelligence*, 2002, Vol. 46, No. 3.

Kober, Stanley,"Why Spy? The Uses and Misuses of Intelligence", *Policy Analysis*, December 1996.

Krouse, William, J. and Perl, Raphael F., "Terrorism: Automated Lookout Systems", *Congressional Research Service* (RL310919), 18 June 2001.

Lowenthal, Mark, M., *Ethics of Spying: A Reader for the Intelligence Professional*, CQ Press (Congressional Quarterly Press), 2006

Lowenthal, Mark M., *From Secrets to Policy*, CQ Press, 2012.

Pease, Bruce, *Leading Intelligence Analysis: Lessons from the CIA's Analytic Frontlines*, CQ Press, 2019.

Riebling, Mark, *Wedge: The Secret War Between the FBI and CIA*, New York, Alfred A. Knopf, Simon & Schuster, 1994.

Rosenzweig, Paul, and Kochems, Alane, Risk Assessment and Risk Management: Necessary Tools for Homeland Security, *Heritage Foundation*, Backgrounder No. 1889, 25 October 2005.

Treverton, Gregory, F., "Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons", *Intelligence and National Security*, 2003 Vol. 18, No.4.

DOI: 10.19165/2020.6.0120

Web Resources

CIA Freedom of Information Reading Room. Available at: cia.gov/library/readingroom/home.
Department of State, Freedom of Information Reading Room. Available at: https://foia/state.gov/search/search.aspx.
FBI vault. Available at: www.vault.fbi.gov/.
Loyola.edu/dept/politics/intel.html.
National Security Agency Freedom of Information Reading room. Available at: nsa.gov/resources/everyone/foia/reading-room.
Studies in Intelligence at CIA. Available at: https://www.cia.gov/resources/csi/studies-in-intelligence/.

DOI: 10.19165/2020.6.0120