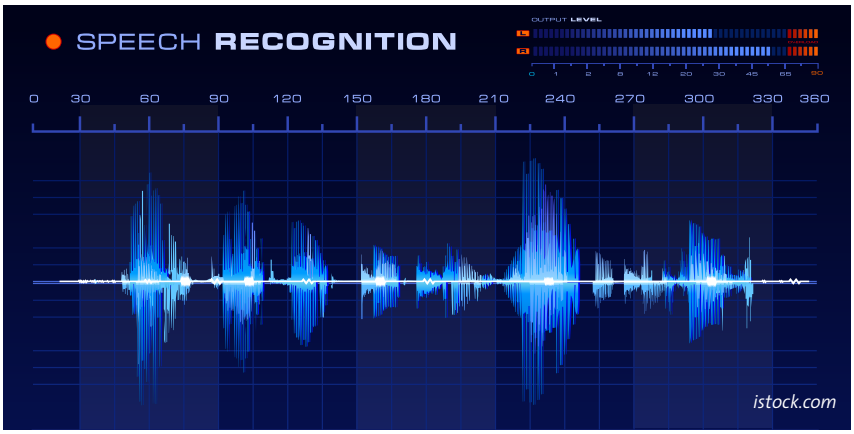
CSS Analysis in Security Policy

CSS ETH Zurich

No. 82 • October 2010

INTELLIGENCE AGENCIES: ADAPTING TO NEW THREATS

Following the end of the Cold War and the 9/11 attacks, terrorism has become the foremost concern of Western intelligence agencies. Efforts are being made to enhance resources and legal powers for information collection, and data sharing has increased. However, implementation of these measures faces continuing hurdles. Furthermore, intelligence agencies are confronting new challenges from state actors, which contravene ongoing trends in intelligence adaptation. Horizon scanning for new threats is therefore required, in order to avoid strategic surprise.



The end of the Cold War in 1989 disorientated intelligence agencies across the world. Accustomed to monitoring security threats against a backdrop of Great Power rivalry, they suddenly had to redefine organisational missions. In the West, such agencies no longer had a 'main enemy' against which to focus intelligence collection, and began adding new issues to their list of intelligence targets. The net effect was to stretch intelligence resources, in both collection and analysis, to an extent that made coverage superficial. Accompanying this trend was a revolution in open source intelligence. As countries within the former Soviet bloc democratised, intelligence analysts were swamped with data from previously 'denied' regions, at a rate which exceeded their capacity to monitor.

Meanwhile, non-state actors were unobtrusively empowered by globalisation, which allowed them to study their external environment and adapt accordingly. One of these was al-Qaida. Many of its founding members were already familiar with intelligence techniques, having been pursued by Arab security services since the 1980s. After finding sanctuary in Afghanistan in 1996, they combined this knowledge with strategic reconnaissance to plan attacks upon the West. Although their activities were monitored by Western governments, the latter could not acquire 'actionable' information about terrorist plots. This failure hit home on 11 September 2001.

Terrorism as a conceptualiser

Since 2001, terrorism has had two direct impacts on Western intelligence. One is to compel governments to increase agency resources and legal powers, and the other is to enhance information sharing domestically and internationally. To take the former aspect first: the attacks have focused collection efforts onto a common threat once again – international terrorism. The analytical drift which characterised threat assessments during the 1990s is gone. Violent transnational actors, foremost of which is al-Qaida, have become the new 'main enemy' and fill in the role previously held by the Soviet Union. A massive effort is underway within Western states to build capabilities that would optimise intelligence agencies for the detection, pursuit and neutralisation of terrorists.

As part of this process, intelligence resources have been increased. Between 2001 and 2006, the Central Intelligence Agency's clandestine service tripled in size. The Federal Bureau of Investigation increased its analytical cadre by 100%. Britain's security service MI5 has more than doubled in size from 1,800 personnel in 2001 to approximately 4,000 today. However, the expansion has been accompanied by problems. MI5 has met with limited success when recruiting among religious minorities, the very groups whose support is most essential to counterterrorism. In 2007, only 5% of its staff came from a minority background. The CIA and FBI face an even more serious challenge: that of terrorist penetration through Arab-speaking double agents. In one case, a Lebanese-origin CIA official was discovered sending classified data to the militant group Hizbollah. Such developments indicate a need to balance proactive intelligence collection with organisational security.

Also, as part of the new focus on counterterrorism post 9/11, intelligence agencies have been given enhanced legal authority for domestic technical surveillance. This has led to concerns about privacy viola-

tions; concerns which are yet to be fully resolved given the clandestine nature of technical interception. In any case, privacy infringement is integral to surveillance, due to the 'domino effect' of interpersonal connections. For instance, although 125,000 Italian citizens were subjected to legally-authorised wiretapping in 2007, the actual number of people recorded was closer to 1.5 million, since each target would speak with nearly 50 different people.

Hoping to prevent civil rights violations by intelligence agencies, many governments have introduced oversight processes, or strengthened existing ones. France has placed its intelligence community under nominal parliamentary oversight, while Britain has strengthened its oversight mechanism in response to public scepticism over the integrity of intelligence processes. Such scepticism stemmed partly from erroneous estimates of Iraqi WMD capabilities, released by the government in 2002 in a bid to boost public support for war. Given that the United States has a much more elaborate system of legislative oversight and yet could not prevent the politicisation of intelligence prior to the 2003 Iraq War, there is little reason to believe that misuse can be completely avoided.

Comparing the US intelligence system with those of European states is generally difficult, due to the much bigger scale of American intelligence resources and policy concerns. There are differences in counterterrorist policies as well. The US security establishment views terrorism as a predominantly foreign terrorist threat, with only about one in every 30,000 American Muslims thought to be susceptible to jihadist propaganda. Accordingly, it has focused on protecting the US homeland by immigration control and computerised profiling. Its vast technical collection apparatus, capable of intercepting 1.7 billion electronic communications daily, constitutes the vanguard of counterterrorist efforts. The CIA meanwhile, is hunting down terrorist cadres overseas, including through drone strikes in Pakistan. European governments on the other hand, perceive terrorism as a more home-grown threat. As a result, their counterterrorist efforts are more domestically-oriented and rely heavily on police informers. These serve as tripwires for detecting pockets of radicalisation. There is also no policy of targeting terrorist leaders abroad through covert strikes.

Information sharing

Another major impact that 9/11 has had on intelligence structures is in information sharing. Critics have pilloried the CIA for not watchlisting two of the al-Qaida terrorists involved in the attacks, about whom it had previously collected information. The lapse has been attributed to turf warfare, feeding a belief that failures of 'dot connection' allowed the attacks to occur. Accordingly, efforts were made to consolidate counterterrorism data, resulting in the formation of the Terrorist Threat Integration Center in 2003 (renamed the National Counterterrorism Center in 2004). The FBI has also expanded its domestic and overseas presence, setting up fusion centers within the US and adding 31 overseas liaison offices to the 44 which already existed in September 2001.

Britain has followed suit, establishing the Joint Terrorism Analysis Centre in 2003, and developing Regional Intelligence Centres across the country, where MI5 staff pool information with local law enforcement. Since the vast majority of its counterterrorism cases have overseas components, MI5 cooperates extensively with the Secret Intelligence Service and General Communications Headquarters (the British foreign intelligence and signal intelligence agencies). Germany has mirrored these developments, creating a Joint Counterterrorism Center in 2004 that facilitates information sharing between 40 federal and provincial security agencies. Since 2007, it has been operating a Joint Anti-Terror Database which pools information from all agencies, both intelligence and police. The Swiss government has gone even further, merging its domestic and foreign intelligence agencies into one monolithic structure in order to facilitate information sharing.

Besides these efforts at consolidating data domestically, initiatives have been set up to facilitate information sharing at bilateral and multilateral levels. These have met with mixed success. At the bilateral level, intelligence liaison is plagued by latent clashes of interest. Currently, arrangements exist to share time-sensitive warnings on specific terrorist plots, but little progress has been made in sharing operational-grade information for offensive use. A partial exception here is Pakistan, which under diplomatic pressure has cooperated with the CIA in pursuing terrorist leaders.

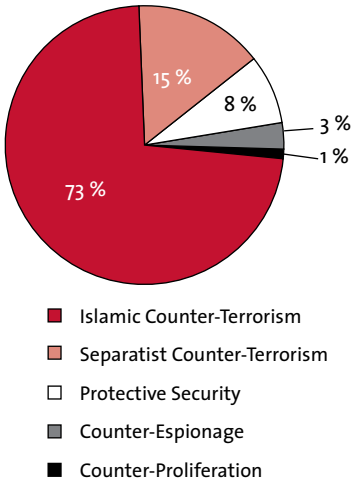
At the multilateral level, European governments have been prompted to share information on terrorism, organised crime and immigration, not least due to the loosening of border controls within the European Union and adoption of a common currency. The most important forum for intelligence cooperation is the Berne Club, which was established in 1971 and currently brings together intelligence chiefs of 27 countries (most EU member states plus Norway and Switzerland). The Club has its own communications network and facilitates joint training of intelligence personnel. An independent body established in November 2001, known as the Counterterrorism Group, also includes the United States as a member. The Group aims to create a biographical database of suspected terrorists and criminals within Europe. Although this is a positive step, experts believe that the group's deliberations have thus far had little policy impact, and that even information sharing is limited. Intelligence agencies of larger European states in particular, are reluctant to share information with smaller partners since they get little in return.

There is also reason to doubt whether the above-described measures will suffice to prevent the continued evolution of terrorist threats. Al-Qaida and its affiliates are now exploiting a new vulnerability that has appeared in Western intelligence systems since the 1990s: information overload. The consolidation of data is threatening to overwhelm even the expanded analytical capabilities of intelligence agencies, making it likely that warning signs of an attack will not be interpreted in time. By flooding analysts with misleading electronic chatter, terrorists can generate 'noise' that would disguise the signals pertinent to an impending attack on Western targets.

New and re-emerging threats

Even as counterterrorism consumes the bulk of policy attention and intelligence resources, fresh tensions are emerging between state actors. Spy scandals and frequent attacks by Chinese hackers have convinced Western intelligence agencies of the need to refocus attention on counterespionage and information security. The latter means that the 'need to share', hitherto considered a credo of the 21st century intelligence environment, could be replaced by the more traditional 'need to know'. Furthermore, conventional methods of intelligence collection, long considered outdated or unsuitable for counterterrorism, might return in a modified form.

MI5 resource allocation, 2010



Source: www.mi5.gov.uk

Foremost among these is signals intelligence. Established wisdom holds that intercepts are of limited use against terrorist groups. The latter are supposedly more vulnerable to human intelligence and psychological operations guided by open source intelligence. Irrespective of whether this is true, the return of state versus state competition suggests that technical collection will remain central to intelligence activities. Espionage conducted under commercial and diplomatic cover is also likely to return to the levels of the Cold War. This is in part due to the global power shift from West to East.

Emerging powers such as China are believed to be using both human and technical sources to acquire commercial secrets from Western businesses. They have been aided by the proliferation of digital technology, which permits the surreptitious copying of corporate records onto electronic storage devices. Such information, once stolen, can be passed on to either rival companies or foreign governments. In the case of China, the two are often intertwined, given the Chinese military's substantial business interests. Furthermore, globalisation itself has facilitated the process of knowledge transfer. According to one rough estimate, 60% of the secret information collected by foreign intelligence agencies comes through sources inside the local offices of multinational corporations.

The low labour costs of many developing countries, coupled with their growing expertise in science and technology, make economic espionage a long-term threat to Western societies. By stealing trade secrets, state-supported businesses across the world can bypass years of wasted research and produce under-priced goods that Western ones cannot compete with. They can also rig competitive tenders in their favour, through cultivating decision-makers within the relevant governments. It would be incorrect however, to presume that the threat is limited to developing countries. In the current economic climate, with Europe reeling under an unprecedented austerity drive and slow economic recovery, the temptation to engage in economic espionage is likely to prove overwhelming for some governments.

Not only is such espionage damaging to domestic business, but it potentially has military implications, given that many technologies have both military and civilian uses. A great deal of scientific research remains unclassified in its initial stages, so as to benefit from similar research being conducted elsewhere in the world. During this phase, designs for a promising new technology can be copied with relative ease by an employee with only minimal security clearance. Many recent spy cases in the United States have involved naturalised immigrants and foreign scientists, who have passed on non-classified data to their countries of origin.

This trend poses a challenge for intelligence agencies, since it does not fit into the systems and processes that have been established post 9/11. Human intelligence efforts aimed at penetrating al-Qaida take place in vastly different geographic and cultural milieus from economic espionage. Suspect profiles differ considerably, and efforts have to be made to lockdown data in the private sector. As part of such efforts, MI5 has recently warned 300 British firms that their cyber-infrastructure is vulnerable to attacks by Chinese hackers. Such attacks cannot be easily attributed to state sponsorship, thus complicating the task of fashioning a policy response. Combating both, states and non-state actors simultaneously, is likely to prove challenging for intelligence agencies, especially considering political pressure to focus on the latter.

Given the dependence of modern governments and militaries on computer systems, particularly in the context of network-centric warfare, cyber-espionage is likely to pose a serious security risk. This emerging threat would have multiple dimensions, being able not just to disrupt command and control systems during wartime, but also steal sensitive diplomatic and political data during peacetime. Countering it would require intelligence agencies to recruit technical specialists who can command large salaries in the private sector, and whose skills would therefore, be costly to retain.

Strategic tradeoffs

Given the global economic downturn and fading public memories of 9/11, there are doubts whether the large intelligence budgets of the last decade are politically sustainable. A search is on for ways to optimise the allocation of intelligence resources, such that short-term concerns do not crowd out long-term perspectives. Hitherto, a common criticism of intelligence agencies has been that they failed to engage in strategic analysis of the al-Qaida threat during the 1990s. A similar process might now be underway, as an all-consuming focus on terrorism causes tactical intelligence on the subject to dominate at the expense of horizon-scanning for new threats.

With many European governments cutting back defence expenditure, military power is being gradually replaced by intelligence power as the currency of *Machtpolitik*. Anticipating threats and pre-empting them is becoming central to national defence policies, in contrast to the Cold War when the emphasis was on building large retaliatory capabilities. Although Western intelligence agencies have been reasonably successful in preventing large-scale terrorist attacks since 2001, they shall still need to adapt to changes in the international threat environment if they are to avoid being surprised again. As long as this environment remains fluid, intelligence agencies will have to be dynamic in responding to the operational challenges that it poses.

Author:
Prem Mahadevan
mahadevan@sipo.gess.ethz.ch

Responsible editor:
Daniel Möckli
sta@sipo.gess.ethz.ch

Other CSS Analyses / Mailinglist:
www.sta.ethz.ch

German and French versions:
www.ssn.ethz.ch