2014
HALIFAX
PAPERS

HALIFAX
INTERNATIONAL SECURITY FORUM

NOVEMBER 21-23, 2014

GET SMART: GAINING INTELLIGENCE, MISSING THE MEANING

— Baroness Pauline Neville-Jones

Today, intelligence has taken a central role in all aspects of national security at home and abroad. It is a new condition that is unprecedented in Western democracies and arises directly from Islamist extremism that has found its latest haven in an increasingly inflamed Middle East.

In its terrorist and criminal form it is a serious security risk. Even in its nonviolent, ideological form, it is a threat to liberal democratic values, which it seeks to overturn. Its tentacles reach into the streets of communities thousands of miles away.

Using electronic communication and simple organization, terrorists can both recruit and inflict loss of life quite cheaply.

The resources that have to be brought to bear to pursue the perpetrators, to protect society against them, and to counter their vile message on the other hand, are very extensive. Moreover, since reliable overt channels of communication are not a feature of terrorist movements, governments are left uncomfortably dependent on intelligence as the primary, if not sole, uncorroborated, source of information for policy making.

On the face of it, this dependence on intelligence would seem to argue for further investment in technological development and expansion of already ballooning budgets. One day, quantum technology will emerge from its research phase.

But while we remain in the digital world, Agencies will certainly need to continue to develop and safeguard their cryptographic, including vital interception, capabilities. Beyond that, however, a bigger bang for the buck is more likely to be attained from deploying existing capabilities more effectively: integrating intelligence products more closely with other aspects of policy, while at the same time ensuring its integrity.

In the second Gulf War, outdated intelligence, lack of ability to test agent information against other sources, and misinterpretation of apparent battlefield evidence contributed to policy failure.

Misusing intelligence to drive political argument, as in the UK's "dodgy dossier" over Iraq, left a legacy of mistrust that adversely affects policy options to this day. The value – and the reputation – of intelligence depends on the way it is produced and used.

The stated aim of containing, degrading, and destroying ISIL in Iraq and Syria is urgent and ambitious. Success depends to a considerable extent on building/rebuilding intelligence assets on the ground.

This means using special forces and training local agents who can be deployed in combination with other intelligence, and military and political assets. Early visible outcomes will not be on offer in this painstaking task, which should cover other friendly Middle Eastern and Gulf countries ahead of a further shift of fighters as they begin to be squeezed.

As the base is laid, however, the speed of degradation should accelerate. It should help cut at one of its sources, the poisonous propaganda stream, and disrupt the two-way flow of recruits. The flow will not stop, however, until Agencies in countries of recruitment and passage have developed much greater situational awareness of their domestic security scene, have speeded up exchange of information, and are operating much

more effective border and policing controls than is the case currently.

And, unless there is going to be wholesale resort to executive detention, which tends to create martyrs and is ultimately unsustainable, police must be trained to obtain evidence that is both usable in court and robust enough to obtain convictions.

Developing a sense of shared mission with minority communities is vital since it is within them that a good part of the still grossly underdeveloped work of de-radicalization or, better, prevention of radicalization, has to take place.

In many countries, Agencies could make a much more significant contribution than is presently the case. Intelligence drops onto the cutting room floor unused because its value to those parts of government tasked with identifying the purveyors of ideological extremism is not recognized simply because – rightly – it is not part of the Agencies' own remit.

It makes no sense, however, for government to devote extraordinary resources to overcoming the violent effects of extremism while neglecting to exploit intelligence available about fundamental drivers. Terrorism poses public authorities with a challenge that most find very hard to meet: effective information sharing and coordination of the instruments of policy both internationally and domestically right across departmental stovepipes and into communities.

Without that, a lot of intelligence will be wasted.

Governments have already had to alter laws and institutions to release the capabilities of the state to meet the threat. The focus on domestic security has brought controversy with it.

Paradoxically, the more the governments succeed in threat reduction and the less apparent the threat, the more onerous can seem the accompanying invasion of privacy and constraints on civil liberties.

The ability to scan and collate data communications nevertheless remains vital, and the way forward cannot lie in blocking it so much as ensuring that the legal framework is clear and accountability rigorous; that Agencies are tasked only to genuine priorities; and that the processes involved in producing and using intelligence are operated proportionately.

Bringing about greater transparency will be the best antidote to a corrosive belief in the existence of Big Brother. This is a long haul and the state has to make itself fit for purpose.

Baroness Pauline Neville-Jones is Chairman, Cyber Security Advisory Panel to the Bank of England.