Securing the State: National Security and Secret Intelligence

By David Omand

Consider the artist Michelangelo standing in front of a block of Carrara marble rough-hewn from the quarry. As he later described that moment, "I saw the angel in the marble and carved until I set him free." Sculptors need the patience to recognize that many small steps will be needed to realize their vision. The sculptor needs a strategic sixth sense that can continuously adapt the design to the conditions of the material while testing whether each small incision, however immediately appealing and easily achieved, will end up weakening the final structure. The sculptor needs the confidence to know that the design can be adjusted in response to the inevitable small slips and misjudgments made along the way. Call it the ability to hold the desired ends in mind while being continuously aware of the ways open for achieving them and the means that are at hand. Even the most technically skilled sculptor equipped with the sharpest chisels needs to have a clear sense of the end state – to see at the outset, "the angel in the marble" – that could be the final result of all the labor to come. That is the strategic cast of mind needed for planning modern counter-terrorism.

In building a strategy for countering a terrorist threat there are certainly enhanced means available to governments today. The latest defense equipment technology – from advanced night vision devices, multi-spectral imaging, real time imagery fusion, all the way to high endurance drones armed with high precision missiles – gives forces assigned to counter-terrorism missions a reach and clout and an ability to shape the battlefield unimaginable to previous generations of warriors. New digitized sources of intelligence provide unparalleled insights into the movement and activities of individual suspects and their networks both domestically and overseas. At a tactical level there are these many new tools and much to be learned about how best to apply them.

Yet, these very reassuring strengths can lead to a pursuit of immediate gains only to find later

Professor Sir David Omand, GCB, is a visiting professor in the War Studies Department at King's College London. In 2002, he was appointed to be the first UK Security and Intelligence Coordinator, and Permanent Secretary in the Cabinet Office.

that they may be at the expense of risking longer-term goals. Measures taken with the best of intentions to neutralize terrorist threats overseas can through collateral damage build long-term hostility and provide propaganda opportunities that help breed future threats. Local security clampdowns on minority communities can discourage the flow of information to the authorities. Providing overseas military support for combatants against today's adversaries can end up arming tomorrow's enemies. Domestic security measures (such as restrictions at airports and major events) can over-tax the patience of the public. The search for pre-emptive intelligence on suspect individuals can lead governments into disproportionate intrusion by agents of the state into personal privacy and private life. The understandable desire to find ways of bringing terrorists to justice can strain the limits of the rule of law. In sum, there comes a point when the search for even greater security becomes burdensome and oppressive, and when the public will cavil at what it is being expected to give up to provide it. Yet, the public rightly sees the provision of security as government's first responsibility: government cannot avoid these dilemmas.

How Much Security is Enough?

It is thus not just the choices of ways and means that can be problematic, but also of the ends of counter-terrorism strategy. In essence, the issue again today, as for many countries in the past, is how much security is enough? How can government best set out to exercise its primary duty to protect the public in the face of a substantial terrorist threat, and yet also maintain civic harmony, uphold democratic values and promote the rule of law at home and internationally? The initial need to combat the jihadist terrorist campaign at home and abroad justified itself, robust measures have been taken and have reduced the immediate threat. The harder policy question that is now arising is in relation to the longer-term ends of counter-terrorism strategy: how much security do we think will be enough, in a world of competing priorities for government attention and resources and where terrorism, however dramatic, is only one of many risks facing the public that have to be managed?

In the UK, an all-party consensus has held now for over a decade over what should be the objective of the UK national counter-terrorist strategy (CONTEST, short for COuNter-TErroism STrategy).[1] When we started work on the strategy after the 9/11/01 attacks on the U.S. we debated whether its ends should be couched in terms of defeating or eliminating terrorism. We concluded such an aim was unrealizable since terrorism would inevitably remain an asymmetric tactic of choice for violent extremist groups, and no government can ever give a complete guarantee to the public that terrorists might not at some point be able to slip below the security radar however sophisticated it is. Absolute security is a chimera. Instead, we focused on ways of denying the jihadist terrorists what they most seek which is to shock and disrupt and thus erode public confidence in the ability of government to protect them. The narrative was of fortitude and resilience, setting the objective as a vigorous, collective and communal effort to sustain the normality of everyday life. The formal aim of CONTEST – which *is* being achieved – is therefore to reduce the risk from terrorism so that people can go about their normal life freely (that is, with the rule of law upheld and without the authorities having to interfere with individual rights and liberties) and with confidence (for example, with people still travelling by air and on the underground, visitors vacationing in the UK, with financial markets stable and so on).

The Thermodynamics of Counter-Terrorism

In that way, by stressing the goal of normality in a resilient society, the UK strategy tries to avoid the trap that terrorists set of "the propaganda of the deed," seeking to radicalize supporters through exposing supposed fragility in Western societies and provoking over-reaction from the security authorities. That is one of the eternal security lessons we

should have absorbed (and learned the hard way over the years) about what could be described as the "thermodynamics" of counter-terrorism.

For there is an important relationship between the necessary vigor of security measures imposed to stop terrorists and the intrusiveness of measures taken to obtain intelligence to prevent attacks, and the level of confidence among different sections of the community in the government's commitment to protect the liberties and rights of the citizen. The right to life of the ordinary person in the face of murderous terrorism on the one hand is in tension with the right to privacy of personal and family life on the other. As with the thermodynamic relationship between the volume, pressure and temperature of a gas, too sudden an application of force to compress it and the temperature may rise dangerously to explosive levels; too little pressure applied and the gas is uncontained and will expand out of control. The best approach may well be to cool things down as you gradually build up the pressure, and certainly not to do things unnecessarily that heat it up: the impact of the occupation of Iraq on domestic radicalization in the UK and elsewhere comes to mind; the impact of an Israeli attack on Iran's nuclear facilities were one to occur would be another.

Such an analogy to thermodynamics cannot be pushed too far–the point to be registered is the inter-relationship between a nation's security effort in the face of domestic threat, the direct effect on the risks faced by the public, and the indirect effects on the rule of law, civil liberties, human rights and thus civic harmony or *Civitas* – the public value of harmony in the community based on a shared sense of place, of belonging, regardless of ethnic roots or religious difference. The choice of security strategy is of course crucial to getting that thermodynamic judgment right.

This is not just a contemporary issue. It is a recurring dilemma experienced by governments over the centuries. I titled my book *Securing the State,*[2] and illustrated it with details from a remarkable attempt almost 700 years ago to describe the balance needed for good government. Ambrogio Lorenzetti's great 14th century fresco cycle in Siena in Italy, entitled Good and Bad Government, illustrates that some of the most pressing dilemmas we face over public security are ancient ones, such as the balance between security and the rule of law, albeit today disguised by the effects of modern technology.

Good government today as in that 14th century vision brings peace, stability and security, prosperity, and culture. The painting shows cheerful townspeople and country folk working in harmony and going freely about their affairs transporting their goods on well-kept roads or sowing in the weed-free fields. Builders are hard at work developing the city-state. The watchtowers are well kept and manned.

Hovering overhead in the fresco is a winged figure, labeled Securitas, or security. The winged figure also holds up a scroll on which is written the promise that under her protection all can live in safety, and without fear: the words eerily presage the aim of CONTEST, the UK government's 21st century counter-terrorist strategy, "so that people can go about their normal business, freely and with confidence."

On the other hand, in the fresco representing bad government, the figure of Tyranny dominates. The prevalent emotion is insecurity and fear. Not only are the city walls crumbling, leaving the city vulnerable to its enemies, but the very internal fabric of the town is decaying. The message directed at 14th century Siena's rising merchant class (and now to our own global markets) is that insecurity makes investment and thus innovation hazardous.

In a nutshell, the argument is that good government will always place the task of "securing the state" at the top of its priorities. With security come confidence, economic and social progress and investment in the future. But good government also recognizes, as the 14th century frescoes show, that security needs the active support of all sections of the public and thus the right relationship between justice, civic harmony, wise administration, fortitude, prudence and the other virtues to which the wise ruler and government should aspire.

New Strategic Imperatives

It is tempting to be deflected from such a train of thought by the obvious features of modernity with which we have to grapple. There are new security lessons we have to learn from recent experience, such as the impact (for good and ill) we must now expect from the ease of international travel (of capital as well as people), and the openness of our society to global influences not least through the Internet and social media. Rightly it has been said that abroad has come home, and threats originating overseas can quickly affect domestic security spaces. And the reverse is also true: an offensive cartoon gets published or an insult perceived to sacred scriptures, and an embassy burns overseas.

The strategic narrative governments choose to tell about today's terrorism has to provide a satisfying explanation to the public of why they are at risk, of the historical developments and ideologies that have sustained this threat (recalling that to understand is not to excuse or condone). The explanation has not just to highlight the characteristics of specific emerging threats to warn the public of them. The narrative must generate support for the measures being taken – and in some cases, not being taken – to counter the threat and public acceptance of the residual risk that will remain. It has to incorporate, to use the term being popularized by King's College Professor Sir Lawrence Freeman, "the strategic narrative" government chooses to believe about what is going on in the world, including about the character of the enemies of the state.[3]

As an illustration consider the way that the surprise attack on the U.S. of 9/11/01 created new narratives. On the one hand, 9/11/01 reinforced a growing view in both the U.S. and the UK that not only should states obviously be prepared to use force to defend themselves against external attack by other states, but in the face of this kind of extreme suicidal terrorism governments have a responsibility to their citizens to anticipate trouble brewing and to act before it is too late. It is in the nature of many of these threats – mass murder and suicide bombings, or terrorists armed with a dirty bomb, for example – that we cannot afford to wait until the enemy is at the gates, or even inside the city, before taking action to safeguard the public. This thinking has led to policies intended to deal with potential trouble upstream and far from our shores. Interventions have extended to direct military as well as diplomatic intervention to help the governments of countries not able to protect their citizens and whose instability threatens our own security, with the rediscovery along the way of counter-insurgency doctrine and its development for modern times.

On the other hand, however, the strategic narratives told after 9/11/01 by the U.S. and the UK about the ends of counter-terrorism have been subtly different. For the U.S. America had been the subject, as at Pearl Harbor, of a savage surprise attack from overseas. As President Bush's national security strategy subsequently stated, America is at war, thus reflecting al Qaeda's own characterization of the external aggression against the U.S. as war. This metaphor has legitimized abnormal "wartime" measures, first embodied in the Bush "War on Terror," aimed at identifying and destroying the external enemy, al Qaeda.

For the UK, the jihadist threat, although inspired and directed from outside, had early on a domestic dimension, with jihadist extremism gaining pockets of support in some domestic communities within the UK with strong connections both to Pakistan and to North Africa. In the course of gathering funds and recruits to support jihadist activity overseas, quite apart from the few extremists actually engaging in terrorist planning and conducting attacks within the UK, the criminal law was being broken. The first signs of this jihadist terrorism inside the UK also coincided with the final throes of the Provisional IRA's bombing campaign in London. A domestic law enforcement model therefore dominated the government narrative, stressing the need to bring terrorist suspects before the Courts, and to prosecute them for a range of terrorist and related offences. Unlike a war metaphor seeking defeat of the external enemy, the

UK CONTEST counter-terrorism strategy had the formal aim of reducing the risk from international terrorism with the objective of maintaining domestic normality – so that people could go about their everyday business, freely and with confidence. For the UK, the legal framework has therefore been international human rights law (the European Convention on Human Rights was incorporated into UK domestic legislation in 1998); for the U.S. it has been the international humanitarian laws of war that have governed the attack on senior al Qaeda members and associates regarded as enemy combatants wherever they are.

These strategic differences across the Atlantic may seem abstract, but they have had practical consequences (for example in differing rules of engagement for the handling of prisoners in Iraq and Afghanistan) that have had to be managed within the very closeness of our deep relationship with the U.S. Our invaluable transatlantic intelligence cooperation grows closer than ever and our joint military operations overseas continue, but there will inevitably continue to be occasional difficulties when the actions and methods justified by these different narratives collide.

Strategic Logic of UK Counter-Terrorist Strategy

The UK CONTEST counter-terrorism strategy has remained in force now ten years after its initiation and is on its third major iteration under its third Prime Minister.[4] One of the reasons the strategy has lasted is that it incorporates the logic of risk management. To achieve the state of normality that is its goal there are campaigns to influence each factor in the risk management equation that provides the measure of total risk: likelihood, vulnerability, initial impact, and duration of disruption.

Thus, the strategy aims to make attacks less likely by improving the intelligence and law enforcement capability to uncover terrorist networks and frustrate attacks and bring terrorists to justice (what in CONTEST was termed the Pursue campaign); it aims to reduce the incidence of radicalization in the community and overseas to stem the flow of terrorist recruits (the Prevent Campaign); to reduce the vulnerability of the critical civil infrastructure on which society depends including aviation (the Protect Campaign); and to equip and exercise the emergency services to reduce the impact should terrorists succeed in mounting an attack (the Prepare Campaign). The value of such continuity of basic strategy in terms of maintaining effective counter-terrorist effort, not least during the run-up to the recent Olympics, should not be underestimated. I judge it a success in its own terms: as the 2012 Olympics showed the UK is a nation living in peace, despite the continuing substantial level of threat from militant jihadist extremists.

This risk management approach has now been extended in the UK beyond countering terrorism. When the current British coalition government published its overall National Security Strategy,[5] it spelled out those major modern threats and hazards that have to be managed, from terrorism to cyber piracy, and from instability in key regions overseas to natural disasters, as well as the continuing task of preserving the territorial independence of the United Kingdom, not least through our membership in NATO.

The National Security Strategy identifies four "top tier" risks:

- international terrorism affecting the UK and its interests overseas;
- hostile attacks upon UK cyber-space;
- a major accident or natural hazard;
- an international military crisis drawing in the UK.

Since these priorities were identified two years ago, examples of all four risks have occurred. Al Qaeda in the Arabian Peninsula (AQAP) in Yemen for example almost brought down airliners with bombs hidden in printer cartridges discovered at

Luton airport in the UK; Al Qaeda in the Islamic Maghreb (AQIM) murdered British workers when they attacked the major gas facility operated in part by BP in Algeria. Severe persistent advanced cyber-attacks from China and elsewhere are a daily occurrence. The Libyan crisis saw British Armed Forces in action in a new theater. And although the major environmental disaster happened in Fukushima, Japan, the repercussions in the global industrial supply chain were quickly felt.

A characteristic of many such risks is of course that they are as the economists say, exogenous: their origins cannot be controlled by any one country such as the UK, and they are hard to predict; but in many cases their impact can be moderated by prior preparation. What the hard and dedicated work of the security and intelligence authorities can therefore do is shift the odds in the public's favor.

A Modern Approach to National Security

This modern approach to national security therefore rests on three sets of propositions.

The first step in the argument is recognition of the implications of regarding national security as a collective psychological state as well as an objective reality such as freedom from foreign invasion. People need to feel sufficiently safe to justify investment, to be prepared to travel, indeed to leave the house in the morning to get on with ordinary life and to live it to the full – even in the face of threats such as terrorism and hazards such as pandemics. Our adversaries – and the international markets – must know we have the confidence to help each other and to do what is necessary to defend ourselves.

Looking at the type of malign threats that impact on our increasingly technologically dependent society, we have to be prepared to invest in advance to prevent attacks, to reduce our vulnerabilities and to invest in higher levels of resilience. In a comparable way, we could tomorrow face the consequences of major natural hazards, such as the effects of "space weather" resulting from coronal ejections from the sun, or animal diseases jumping the species barrier, or those that are likely to flow from resource stress as the global climate changes. Governments need to anticipate and act now – preferably in international concert – to mitigate the consequences of such hazards.

A national UK risk register and matrix to help plan such anticipatory work was developed when I was the UK Security and Intelligence Coordinator, and is now published and regularly updated.[6] The matrix shows the most significant hazards ranked by likelihood (and in the case of malign threats, ranked by plausibility) and a relative impact score, taking into account vulnerability to this specific risk. Of course, such an approach, if it is to be useful, cannot include every very low probability/high impact possibility that might be imagined – the first such matrix did not include either irresponsible bankers precipitating the economic crash or Icelandic volcanic ash clouds disrupting aviation (now added to the register), and there will always be previously unknown unknowns that arise to surprise us. So humility is needed about our ability to predict future disruptive challenges. But it should be possible to give government and the private sector what I term "strategic notice" of possible futures that were they to arise would cause us problems. Such strategic notice can then guide conceptual thinking, research and development into counter-measures, investment in resilience and protection, and not least intelligence gathering and horizon scanning to spot early signs of emergence and crystallization of the risk.

The second step in modern national security strategy builds on that recognition of the citizen-centric view of threats and hazards. We have to accept that we should be aiming for the sensible management of risk, not on attempting to eliminate risks altogether. Efforts to avoid all risk can do more harm than good since the law of unintended consequences often applies to the measures we take. If unreal expectations are generated then failure will breed public cynicism and an accusatory blame culture when things do not turn out

Photo by Ian Visits on Flickr

London Olympics Security Trial

as planned. In particular, as already noted, governments in their pursuit of security can risk compromising freedom of movement and of speech, and the rule of law, thus disturbing the civic harmony that lies at the heart of successful societies. Indeed, an important ingredient in public security in a democracy is confidence in the government's ability to manage risk in ways that respect human rights and the values of society.

The third step in the argument then follows. It is to see that the key to good risk management, maintaining that delicate balance, is to have better informed decision-making by government, and thus place greater weight on the work of the intelligence community.

The overall purpose of an intelligence community can be said to be to improve the quality of decision making by reducing ignorance. Today there is more information available than ever before to help us do that. So-called secret intelligence is simply the achievement of that purpose in respect of information that other people, such as terrorists or rogue states, do not want us to have, and we normally do not want them to know we have. Obviously decisions should be based on adequate knowledge of the situation – situational awareness – plus a deep understanding of the roots of what is going on. With situational awareness plus good explanation of why the situation is as it is, there is some hope that what is liable to happen next can be predicted and risks anticipated, and successfully managed, within the limits of the knowable.

With pre-emptive intelligence, criminal networks can be identified and individuals brought to justice without having to resort to cruder measures – the bludgeon of state power – to try to protect the public as was seen in the early 1970s in Northern Ireland, with mass arrests and internment without trial, house to house searches, roadblocks, and large scale stop and search. An advantage of having adequate pre-emptive intelligence is that by making it possible to reduce the level of threat, political pressures are relieved that otherwise would build up on government to take more draconian measures so as to reassure the majority, but that may alienate the community among which the terrorist seeks sanctuary and support, feeding in to the narrative of the extremist.

Thus intelligence – broadly defined – can be used to improve the odds of achieving our goals beyond what we would have managed had we simply tossed a coin to decide between courses of action, acted on hunch, or allowed events in the absence of decision to decide the outcome. But it is always a matter of odds, not certainties. Since the London bombings of 2005 there have been around a dozen jihadist terrorist plots directly affecting the UK. A few, such as the Haymarket car bombs, the plot that ended violently with the terrorists on the run attempting to crash a car loaded with gas cylinders into Glasgow Airport, failed only because of slip-ups by the terrorists. Most failed because the intelligence services and the police got onto their trail first. We had a trouble-free Olympics in 2012 in London, in large part because of a great deal of pre-emptive work by the security authorities.

Anticipation as a component of national security strategy places a great responsibility on the intelligence officers and analysts who are to provide the strategic and tactical intelligence. Anticipation also places a huge responsibility on the shoulders of those who have to decide whether and how to act upon intelligence, or not. As Machiavelli said, "a Prince who is himself not wise cannot be well advised."

An Effective Intelligence Community

From this line of argument flows a strong case for the increased importance for modern national security of an effective national intelligence community working with its counterparts in like-minded nations. By the term effective is meant an intelligence community that flexibly spans domestic and overseas interests in order to generate actionable intelligence, that works harmoniously with law enforcement and partners overseas to help disrupt threats and bring suspects to justice and that has a well developed analytic capability and the capacity to manage the mass of information and "big data" that modern digital technology makes available.

It is rare that raw intelligence reporting speaks for itself as an unambiguous empirical finding might. Questions of interpretation always arise, and patterns of observed evidence can have widely differing interpretations. Consider how the intelligence analyst might approach a typical question that a policymaker or military commander might pose. To take one example from the arena of current international politics, given the more hawkish rhetoric from the most recent People's Congress about building powerful armed forces commensurate with China's international standing, would the Chinese People's Liberation Army (PLA) be likely to use direct military force in seeking to reverse the Japanese intention to nationalize the disputed territory that Japan calls the Senkaku (and China, the Diaoyu) Islands in the East China Sea?

To answer such a question the analysts can assemble a great deal of information. These days a good situational awareness of the current position can probably be obtained from open sources, possibly confirmed by more sensitive diplomatic or other reporting. But to make sense of the way the situation might develop, the analyst must apply – often unconsciously – some explanatory mental model.

Capabilities and Intentions

Traditionally, many defense intelligence analysts would first try to establish the military capability, and economic and other levers, at the disposal of the parties. In the case of this dispute between China and Japan, this would involve assessing what each side could bring to bear, for example if warning shots were to be fired and the dispute escalate. Then the bolder analysts might try to judge the intentions of the parties towards the dispute and possible escalation. This distinction, between capabilities and intentions, is often colored by an emphasis on capabilities as a guide to policymaking given the recognition that capabilities can take a long time to build up, but intentions can change in the twinkling of an eye or with the arrival of new leadership.

For some purposes, governments do need to assess what might be the worst case they could face – even without detailed intelligence as to intentions – so as to be able to consider how best to protect their national interest in specific ways. This is common in domestic security planning. Thus, stockpiling smallpox vaccine effectively removes the incentive for terrorists to try to obtain and spread that disease; having heavily armed guards at nuclear sites similarly makes what could be a catastrophic attack very unlikely. But a nation cannot afford to act on every possible worst case or always assume the worst of its neighbors. Nor is the worst case usually what intelligence analysts would forecast as the most likely outcome on which diplomats and policymakers should act. This poses an obvious problem of how to respond to a build-up of capability, and in public communication of an assessed threat, in balancing reassurance of the relatively low likelihood of the worst case with warning of the adverse consequences to society were the unlikely to happen. A comparable dilemma often faces government over communication of a domestic terrorist threat: very low risk to any individual; but high risk in terms of the adverse consequences to society as a whole if an attack were to take place.

Distinction Between Secrets and Mysteries

Another model influencing analysts might be the distinction (introduced during the Second World War by Professor R.V. Jones, the founder of scientific intelligence) between secrets and mysteries. Secrets are in principle knowable, since the events in question have happened and decisions have been taken and are in principle discoverable, although no intelligence agency will succeed in uncovering all of them.

But no intelligence source, however well placed, will be able to provide the sure answer to mysteries, since these concern events that have not yet happened and may not happen – the leader has perhaps not decided on his next step, or may not have confided his decision to anyone. Yet, policymakers and military commanders will still demand the intelligence analyst's best estimate of what will happen next. Those customers need to be very aware to distinguish when they are being told a secret – such as the order of battle and states of readiness of the naval and air power the Chinese could mobilize in the East China Sea – from when they are being given the best divination of a mystery – such as whether and in what circumstances the Chinese might fire warning shots at any Japanese Self-Defense Force units approaching the disputed islands.

And the example illustrates the problem with that model of analysis since our best guess at the mystery of whether in certain circumstances Chinese and Japanese leaderships would escalate the dispute depends in part on our judgment of how they would assess the possible wider responses, including from the U.S., UN, EU and regional powers, and how they would affect Chinese and Japanese national interests respectively. So intelligence judgment in such circumstances is a complex exercise in game theory, not just about the interactions of potential adversaries facing each other in a conflict or dispute, or even their capability for action, but about how they view each other and the rest of the world. A complete intelligence assessment of the situation thus also contains an assumption about the likely effectiveness of our own declaratory policies towards the potential conflict. Such interaction of strategic narratives introduces complexity to the old distinction between secrets and mysteries.

Situational Awareness, Explanation, Prediction and Strategic Notice: a Useful Model of Intelligence Analysis

In teaching intelligence studies in London, I offer another related way of organizing intelligence assessment. I suggest three "phenotypes" of intelligence judgment that, together with the concept of strategic notice, form a useful model of modern intelligence analysis.

The three phenotypes are:

- the use of the best validated evidence that can be accessed to provide situational awareness, to answer questions of the "who, what, where and when?" type;

- the best explanation of the causes of events (and the motivations of those involved) that can be devised having examined which hypotheses are most consistent with the evidence and our historical understanding, to answer questions of the "why? and what for?" type, leading in turn to the third phenotype;

- careful prediction of how events might unfold in different circumstances including how all those involved might respond to the measures we and our allies might take, to answer questions of the "what next and where next?" type.

But prediction beyond a short time ahead is inherently problematic, and should be complemented by using the technique of strategic notice: the identification of possible future developments of interest to answer questions of the "whatever next?" type. On this research and development can be commissioned and intelligence gathering requirements set, and policies developed, without necessarily assuming that we can know whether and when such developments will actually occur. We cannot eliminate surprise, but we can learn to live better with it by being less surprised when it happens.

That brief example of the East China Sea is in many ways an old fashioned one for which precedents can be studied; a longstanding territorial dispute between two powerful states that have a history of antagonism. The subjects of intelligence analysis over the last decade have, however, increasingly involved the activities of so-called non-state actors; terrorists, proliferators, narco-traffickers, organized criminals, and cyber hacktivists. Intelligence agencies seeking to uncover covert networks have had to develop new capabilities to track the movements and reveal the communications, air travel, financial transactions, immigration records, and so on of their suspects. The tracking down of Osama Bin Laden in May 2011 was a remarkable example of what I would describe as the emphasis now on, "intelligence for action," against hostile non-state actors – and a pointer to the increasing importance in warfare of having flexible forces able to use tactical intelligence to achieve a strategic impact.

Managing Moral Hazard

PROTINT is my term (by analogy with HUMINT and SIGINT) for the gathering of intelligence from the data-protected personal information about individuals to be found in digital data-bases either in public or private sector hands and located both on the domestic territory and overseas. What some in the CIA call the "electronic exhaust" that we all leave behind as we live our normal lives in a high-tech society becomes the spoor to be followed. It is in the nature of such databases that they will contain mostly information on the law-abiding citizen, thus information on the innocent as well as the suspect. Very recently the explosive growth in the use of social media — Twitter, Facebook, etc. – provides another channel of access to individuals and their preferences, associations and activities and the sentiment of the crowd. Gathering and analyzing social media to assist the authorities in providing public security, what I call SOCMINT[7], is rapidly becoming a mainstream intelligence activity around the world.

These intrusive methods are powerful and they get results. My conclusion is that we must accept both that the modern "protecting State"[8] needs pre-emptive intelligence in order to manage sensibly the major threats to everyday life and that gathering such secret intelligence will involve accepting the moral hazard of risking on occasions harm to others for a greater good. There is, for example, a price to be paid for obtaining intelligence on

suspects moving amongst the general population, and that is some invasion of privacy, just as recruiting agents active in terrorist networks will run the risk of being accused of colluding in wrongdoing.

There is a danger of public misunderstanding of this line of argument as a call for the secret world of intelligence to be empowered to do "whatever it takes" to keep us safe. It does not, however, follow that we have to accept those propositions as a justification for treating intelligence activity as an ethics-free zone. We do not need to accept an assumption that intelligence agencies by their hidden nature are outside the pale of moral consideration. In the end, there needs to be public trust that the intelligence and security apparatus will only be used when necessary for public protection against major dangers. The common sense position that the citizen has a right to expect that the security authorities will use all lawful means to manage the risks from such dangers also supports the contention that public security requires the authorities to balance rights, such as the right to life – not to be blown up by a terrorist bomb – and the right to privacy and family life of the community at large, as well as the rights of those the authorities have to keep under deep surveillance. The balancing act required is within the framework of human rights not between security on the one hand and liberty, privacy and the rule of law on the other.

The extreme example of a balancing exercise is to be found in armed conflict, where the enemy's right to life (and on occasion that of civilians caught up in the inevitable collateral damage of warfare) has to be hazarded for the greater good of the security of the nation. Most of us would recognize the ultimate use of lethal armed force as morally justified in self defense or to prevent worse outcomes in terms of human suffering. The "Just War" tradition deriving from such thinkers as Cicero, Augustine of Hippo and St. Thomas Aquinas has given us tests to apply such as just cause, right authority, necessity, minimum force and proportionality. As the late Sir Michael Quinlan pointed out[9] by analogy, we can have *Jus ad Intelligentiam* and *Jus in Intelligentia* to govern when the recourse to the moral hazards of secret intelligence is justified and to limit the methods employed. This approach can indeed be applied usefully to the oversight of intelligence work,[10] when it comes to justifying the moral hazard involved, by applying a check-list of six principles;[11]

1. *There must be sufficient sustainable cause.*
   We need a check on any tendency for the secret world to expand into areas unjustified by the scale of potential harm to national interests

2. *There must be integrity of motive.*
   We need integrity throughout the whole system, from collection through to the analysis, assessment and presentation of the resulting intelligence to policymakers.

3. *The methods to be used must be proportionate.*
   The likely impact and intrusion of the proposed intelligence gathering operation, taking account of the methods to be used, must be in proportion to the harm that it is sought to prevent.

4. *There must be right authority, including upholding of the universal ban on torture.*[12]
   We need sufficiently senior sign off on sensitive operations and accountability up a recognized chain of command to permit effective oversight. Right authority too has to be lawful.

5. *There must be reasonable prospect of success.*
   Even if the purpose is valid (guideline 1) and the methods to be used are proportionate to the issue (guideline 3), there needs to be a hard-headed assessment of risk to those involved and of collateral damage to others, and not least the risk to future operations and to institutional reputations if the operation were to go wrong.

6. *Recourse to the methods of secret intelligence must be a last resort if there are open or other sources that can be used that do not run the same risk of moral hazard.*

A Grand Security Bargain

To conclude, drawing on the British experience of the last decade, we can sketch out a series of propositions that can serve as the basis for an ethically defensible security strategy, representing a balance of the competing principles and interests involved.

- All concerned, the executive, its agencies, legislators and the public, have to accept that maintaining security today remains the primary duty of government and will have the necessary call on resources.

- The strategic security narrative government chooses to tell about what is going on in the world should be based not just on the assessment of the threat, but also the likely effects of the response, direct and indirect.

- The public should be invited to accept that there is no absolute security and chasing after it does more harm than good. There is a continuing need to learn to prosper in a world of risk (opportunities as well as threats), and thus to understand – and to apply correctly – the principles of risk management. Providing security today is an exercise in risk management.

- There will always be intelligence gaps and ambiguities, but overall the public must be encouraged to recognize that the work of the intelligence and security services shift the odds in the public's favor, sometimes very significantly.

- Effective management of threats thus involves having pre-emptive intelligence to guide the work of the authorities in protecting the public. They have a duty to seek and use secret information to help manage threats to national security.

- The ability to catch terrorists and mount successful criminal prosecutions is essential, but will not by itself sufficiently protect the public, especially when the terrorist is prepared to be a suicide bomber. Using pre-emptive secret intelligence to help disrupt terrorist networks at home and abroad is thus essential to reducing the risk.

- Secret intelligence, because it involves overcoming the efforts of others to prevent us acquiring it, inevitably involves running moral hazard.

- The effectiveness of such secret intelligence rests on sources and methods that must remain hidden. The public must accept that there is no general "right to know" about security and intelligence sources and methods. Freedom of Information legislation has brought greater transparency into the work of government generally, and enabled government to be better held to account, but it cannot be at the expense of public safety.

- We can nevertheless constrain our intelligence activity by an ethical approach that is based on well understood and tested "just war" principles, and that respects human rights including the prohibition of torture. The law enforcement, defense, security and intelligence communities have to accept in turn that ethics do matter; there are "red lines" that must not be crossed.

- If the secrets of terrorists and serious criminals are to be uncovered and their plots disrupted, there will be inevitable intrusions into privacy. These intrusive methods are powerful and they get results. In careless or malign hands they could be abused. So it is essential that the public have confidence that the security and intelligence apparatus of the state is under democratic control, being properly regulated and is being used lawfully for public protection against major dangers.

- Democratic oversight of intelligence activity has to be by proxy. The public right to oversight

of security and intelligence work has to be exercised at one remove, by a trusted group of democratically elected representatives – together with judicial oversight of intrusive investigative powers with the right of redress in cases of abuse of these powers – who can on our behalf be trusted to enter the "ring of secrecy" and to give us confidence that legal and ethical standards are being maintained.

- Some risks will, despite all our efforts, crystallize and thus there is value in pursuing as part of security strategy a long-term national policy of working with the private sector to build up national resilience against a range of threats and hazards, including in cyber-space.

- And of course, government must never forget the importance of having an informed and supportive public that has confidence in the authorities and their methods.

The ancient Greek term *phronesis* describes the application of practical wisdom to the anticipation of risks. *Phronesis* was defined by the historian Edgar Wind as the application of good judgment to human conduct – consisting in a sound practical instinct for the course of events, and an almost indefinable hunch that anticipates the future by remembering the past and thus judges the present correctly; an appropriate description for effective national security and counter-terrorism strategy. PRISM

NOTES

[1] HM Government, *CONTEST: The UK's Strategy for Countering International Terrorism* (London: HMSO Cm 8123, July 2011), available at http://www.homeoffice.gov.uk/counter-terrorism

[2] David Omand, *Securing the State* (London: Hurst and New York: Columbia University Press, 2010).

[3] Lawrence Freedman, *The Transformation of Strategic Affairs* (London: IISS Adelphi Paper 379, 2006).

[4] Earlier versions of the UK counter-terrorism strategy can be found in: HM Government, *CONTEST: The UK's Strategy for Countering International Terrorism* (London: HMSO Cm 8123, July 2011), available at http://www.homeoffice.gov.uk/counter-terrorism HM Government, *The UK's Strategy for Countering International Terrorism* (London: HMSO Cm 7547, March 2009) available at http://www.official-documents.gov.uk/document/cm75/7547/7547.pdf HM Government, *Countering International Terrorism: The UK's Strategy*, (London: HMSO Cm 6888, July 2006) available at http://www.official-documents.gov.uk/document/cm68/6888/6888.pdf

[5] HM Government, *A Strong Britain in an Age of Uncertainty: The UK National Security Strategy* (London: HMSO Cm 7953, October 2010), available at http://www.number10.gov.uk/news/national-security-strategy/

[6] The January 2012 version of the UK national risk assessment can be found at: http://www.cabinetoffice.gov.uk/content/risk-assessment.

[7] See David Omand, Jamie Bartlett, and Carl Miller, *#Intelligence* (London: Demos, 2012) and the same authors' "Introduction to Social Media Intelligence" *Intelligence and National Security*,Vol 27, no. 6 (December 2012).

[8] See Peter Hennessy (Ed.), *The New Protective State* (London: Continuum Books, 2007).

[9] Michael Quinlan, "The Just War Tradition and the Use of Armed Force in the Twenty-First Century", annual lecture of the War Studies Department, King's College London, 25 January 2006.

[10] Omand, *Op. Cit.*

[11] Alan Rusbridger, the Editor of the *Guardian* newspaper has also suggested in his blog that these principles could also be applied to govern the use of intrusive investigative methods by newspapers and other media in the wake of the current allegations of phone hacking by News Corporation papers. See http://www.guardian.co.uk/commentisfree/2011/jul/07/phone-hacking-alan-rusbridger

[12] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec 10, 1984, 1465 U.N.T.S 85. This position is reflected in the offence in the UK Criminal Justice Act 1988, s. 134 which is committed by any public official or person acting in an official capacity in the UK or elsewhere who "intentionally inflicts severe pain or suffering on another in the performance or purported performance of his official duties."

Photo by Nathan Gibbs on Flickr

Alexander the Great