Assessing differences in national security threat perceptions

Numerous countries release security reports and strategies that can be studied for hints of underlying intelligence directions. James Bingham analyses 16 countries to identify convergence and divergence in threat assessment

Key Points
• National security threat perceptions show some substantial differences even among a group of broadly allied countries, such as in attitudes towards epidemiological risk and migration.
• Cyber attacks, terrorism, and foreign espionage are the three threat categories that are almost uniformly considered to be high priorities.
• Factors such as access to intelligence, commonalities with neighbouring countries, and political pressure will all have a bearing on assessment differences.

Many countries publish national security strategies (NSS), intelligence service annual reports, and similar analyses of national threats emanating from both within and outside state borders. These open-source documents are published on official government websites to ensure accountability and as much transparency as possible within an intelligence environment.

Although based on classified intelligence and therefore necessarily sanitised for public release, the weighting applied to a broad spectrum of threats can provide insights into common and divergent perceptions of threat, and also gives indications of possible underlying intelligence direction and collaboration. Jane’s has compiled an assessment of how 16 states perceive a variety of threats to construct a contrasting weighting of these threats against one another and between states.

How these threats form high priorities within groups of countries also hints at the possibility of shared intelligence between these states, forming the underlying rationale for such similar assessments.

Intelligence sharing and priorities

Although the most comprehensive intelligence-sharing framework across the 16 countries (listed in the accompanying graphic) is that of the ‘Five Eyes’ – Australia, Canada, New Zealand, the UK, and the US – other intelligence-sharing structures also exist. The majority of the 16 countries analysed are members of the EU and NATO, both of which have institutionalised intelligence-sharing channels, such as the EU Intelligence and Situation Centre and NATO’s newly instituted Joint Intelligence and Security Division. However, notably, intelligence shared through multilateral institutional channels virtually always consists of sanitised intelligence assessments and not single-source or highly protectively marked reporting.

Although not operating within the EU’s institutions, the Club of Berne is a senior-level intelligence-sharing and intelligence policy forum for selected intelligence and security services of the EU’s 28 states, in addition to Norway and Switzerland. The Counter-Terrorist Group is a part of the Club of Berne that focuses on counter-terrorism intelligence sharing; it indirectly provides sanitised threat assessments for EU policy makers. NATO’s Civilian Intelligence Committee also serves as a
multinational civilian intelligence structure with delegates from NATO member states. Other specialist institutions also share intelligence and information on specific threats, such as the European Counter Terrorism Centre, run by the law enforcement agency Europol.

Intelligence co-operation may allow the assessment of a particular threat to be amplified through the transmission of sanitised intelligence between co-operative states. The sharing of intelligence indicating that a certain threat is of particular concern to one state’s intelligence community could lead to similar assessments when shared with others, producing a ‘clustering’ of states that prioritises the threat over others in comparison to previous assessments.

Conversely, threats may be ‘downgraded’ if a lower-priority assessment is made by one state based on access to high-quality intelligence. However, overall, the case for increasing the prioritisation of a threat based on intelligence is more likely than decreasing it based on a lack of intelligence. This means that there is likely to be a propensity for edging the perceived threat up the prioritisation scale rather than downwards.

**Common threat classes**

Analysing 12 threat classes across the 16 states, three threat classes stand out as common and are consistently regarded as ‘high’: malicious cyber operations, terrorism, and foreign espionage. Of the 16 countries, the threat from malicious cyber operations was uniformly high, with only New Zealand and Australia regarding the threat as ‘medium’. Similarly, the threat from terrorism was high across...
the board, except for in Croatia and Lithuania. Foreign espionage was another high-priority threat class, with 9 of 15 countries regarding it as a high priority and 7 as medium.

The UK’s allocation of resources between terrorism and ‘hostile state activity’ is particularly illuminating. The UK Parliament’s Intelligence and Security Committee’s Annual Report 2016–17, released in December 2017, identifies how 82% of the budget of the UK Security Service (MI5) was allocated to terrorism and 18% to hostile state activity, including espionage, protective security, subversion, and counter-proliferation.

The threat from offensive cyber operations is also regarded as a top intelligence and security priority by the 16 states assessed. This threat class is regarded as a high priority by 14 of these, with Australia and New Zealand regarding it as a medium priority. New Zealand groups cyber operations as sub-sets and methods within other threat classes, such as foreign espionage, as opposed to a distinct category of threat. This is also reflected by the UK and the US through their attribution of offensive cyber operations to Russia in a 16 April 2018 technical alert, with the threat formally classified as interstate rivalry.

Australia distinguishes cyber operations as an independent threat category, and its independent Australian Cyber Security Centre is hosted by, but separate from, the Australian Signals Directorate (ASD) signals intelligence (SIGINT) agency. The country’s Independent Intelligence Review, published in 2017 – not itself a discrete threat assessment, but instead an audit of the Australian intelligence community’s operations – regards cyber operations as both a threat and an opportunity for the country’s intelligence community. According to the review, the threat will grow into a “new array of national security challenges”.

Although generally regarded as a low-priority threat category by nine of the 16 states, epidemiological threats are conversely classified as high priority by Germany, Sweden, and the UK, with Croatia, New Zealand, Poland, and the US regarding this as a medium threat. Given the predominantly open-source, academic nature of the information used to exchange research and identify threat vectors within this category, this divergence is more likely to be a product of differing assessments of the threat in relation to both the roles of the national security establishments of each state and a balancing of more ‘traditional’ security threats against epidemiological threats.

[Continued in full version...]

(929 of 3000 words)

For the full version and more content:

Jane's Military & Security Assessments Intelligence Centre

This analysis is taken from Jane’s Military & Security Assessments Intelligence Centre, which delivers comprehensive and reliable country risk and military capabilities information, analysis and daily insight.

IHS country risk and military capabilities news and analysis is also available within Jane’s Intelligence Review. To learn more and to subscribe to Jane’s Intelligence Review online, offline or print visit: http://magazines.ihs.com/

For advertising solutions visit Jane’s Advertising