Trust in Interstate Intelligence Sharing

https://www.e-ir.info/2020/06/05/trust-in-interstate-intelligence-sharing/

ROBERT DOVER, JUN 5 2020

Trust is at the heart of all intelligence work. That is trust and distrust, loyalty and betrayal, protection and intrusion. Trust is a coin with two distinct sides, and this coin is as valid in interstate intelligence relations, as it is between intelligence officers, as it is between a communications intelligence analyst listening to an audio feed and their certainty in the feed, as it is between an intelligence officer and her human source. The many attempts of western intelligence agencies to systematise source verification, to structure intelligence analysis, and to lean ever more heavily on computer aids has not removed the essential need for human judgement in the business of government intelligence. A system that relies upon human behaviour and the judgments of humans will always be fallible. It will also always pivot around the notion of trust.

The positives of sharing intelligence are often highlighted during the inquiries that follow intelligence failures. The 9/11 inquiry famously concluded that it was the stovepiping of intelligence about the eventual attackers that allowed the US system to collectively possess sufficient intelligence to disrupt the plot against the World Trade Center and other sites, but to not share that intelligence amongst agencies to deploy assets against the threat (9-11 Commission 2004). We should note that novel threats – those whose premise falls outside of our established thinking – have often resulted in strategic shocks (think Barbarossa in 1941, think Pearl Harbor, think AQ Khan and so on, and so forth). These failures have increasingly been attributed to a failure of imagination and a failure of cultural reflexivity: something noted by Matthew Syed in his most recent book, and by me in my response to it (Syed 2019; Dover, 2019).

We should not be seduced by the idea that greater levels of intelligence sharing equates to better outcomes, either for the agency sending material, or the one receiving it. At the strategic level, *Curveball* was a German BND asset, claiming possession of knowledge about Iraqi WMD programmes. This intelligence became one of the key planks in the allied case for war against Iraq, and yet – as we now know – it was unreliable, and provided because of *Curveball's* desire to see the end of Saddam Hussein's regime (Drogin, 2007). The risk here was doubled through the reliance upon international partners to have done the essential vetting, coupled with the desire to publish the information to support the case for war. At the micro-level, the pre-9/11 stovepiping of information was replaced with greater access to intelligence across the community, which in turn facilitated the *Cablegate* release, a strategic shock of a different kind (Brevini et al, 2013).

The act of sharing intelligence with allies can have unintended negative consequences. Shared counterterrorism intelligence between the UK and US was reflexively tweeted – to great anger and disappointment- by the US President in the immediate aftermath of the Manchester stadium attack, something that suggested a poor grasp of intelligence liaison practices (Jones, 2017). Similarly, intelligence sharing between the US and UK during the early phases of the war on terror exposed both parties to accusations of engaging in, facilitating and benefitting from systematic torture, as ably described by Ruth Blakeley and Sam Raphael in their extensive research on the matter (Blakeley & Raphael, 2020). Neither state would have imagined at the time that these practices would have been reported so quickly, leading to awkward questions about political approval and oversight.

The question of who is friend, who is competitor and who is adversary in the intelligence sphere is also contested. Recent case law highlighted that at the tactical level it was possible for the UK state to authorise its intelligence officers and assets to engage in or to forgive illegal acts if that was necessary in the pursuit of a significant

intelligence gain, stretching the public's understanding of the social contract between them and the state. At this level, my enemy is instrumentally and temporarily my friend. At the international level, we see intelligence agencies far freer to conduct parallel diplomacy, which is often useful to those foreign policy officials operating in the open. The partially obscured picture of the ending of the insurgency in Northern Ireland, that led to the 1998 Good Friday Agreement, was that it was initially brokered by intelligence officers, without the knowledge of the government's senior politicians. Such practices do occasionally also produce some questionable declared foreign policy positions: the UK's relationship with notable Middle Eastern interests has seen it turning successive blind eyes to the funding of domestic radicalised movements, and to allowing the exports of weaponry seemingly against its own criteria. The implied social contract in this parallel diplomacy is the continued provision of useful information in exchange for improved conditions.

Being a declared ally of a capable intelligence power does not insulate a state from intrusive attention. In January 2020, The Washington Post and a team of German and Swiss reporters revealed the existence of the US-German Operation Thesaurus / Rubicon which had, through compromised cypher machines, allowed the US to read the government communications of friendly nations, including NATO members, as well as adversary states during the Cold War (Miller 2020). This could reasonably be seen as a breach of trust by those allies who were and are still within NATO structures with the US. At the fall of the Iron Curtain and with enhanced European integration it would have been reasonable for the German government to conclude that the negative repercussions of being caught intercepting the traffic of fellow EU members was too high a price to pay, and could have been why they withdrew from the arrangement.

However, the Echelon Inquiry of 1999, and the Snowden leaks of 2013 merely reinforced the idea that the Five Eyes group of capable intelligence nations remained firmly in the business of snooping on their allies as much as they do their declared adversaries, and presumably do to this day. Trust between these states is, therefore, governed by a well-defined code of security classifications and accompanying protocols about what information can be passed, by whom and how. The trust in that system is held in the adherence to and strength of these protocols. European nations have showed that their trust in these arrangements is conditional, taking – for example – nearly a decade to conclude arrangements with the US over Passenger Name Records.

The current public relations storm around Huawei's involvement in the 5G networks of the Five Eyes nations is precisely around the concept of trust. Can Country A trust that its information or communications passed to Country B are secure if they are passing through Chinese produced equipment? This is a question of trust in the infrastructure. The other prescient and pressing trust issue is between intelligence agencies, their officers, and some elements of the global political elite: those elites who have simultaneously pilloried the intelligence community as partial, and tried to draw them closer into the service of the individual rather than the office, and those who are said to be unreliable or compromised by competitor nations.

Intelligence agencies have historically sought to insulate themselves away from unreliable political leaders, being selective about what they share, and what they rely on. As we continue our 2020 'coronacaster', intelligence agencies have their hands full with the continued success of competitors pushing disinformation, and cyber-disruption, along with deciphering signal from noise in the economic and security space both at home and abroad. Never has it been more difficult to judge whom and what to trust.

References

Blakelely, Ruth & Sam Raphael, 'Accountability, denial and the future-proofing of British torture', *International Affairs*, Volume 96, Issue 3, May 2020, Pages 691–709

Brevini, Benedetta; Hintz, Arne; McCurdy, Patrick, *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, Palgrave: Basingstoke, 2013.

Dover, Robert. 'The importance of Cultural Diversity in Our Intelligence and Security Agencies: A Response to Syed' (https://www.linkedin.com/pulse/importance-cultural-diversity-intelligence-security-agencies-

syed/?articleId=6579658753442889728) 18 September 2019.

Drogin, Bob. *Curveball: Spies, Lies, and the Con Man Who Caused a War*, Random House: New York, 2007.

Jones, Sam. 'May to confront Trump over Manchester bomb intelligence leaks'*, Financial Times*, 25 May 2017.

The National Commission on Terrorist Attacks Upon the United States, *The 9-11 Commission Report*, 2004 (https://govinfo.library.unt.edu/911/report/index.htm)

Miller, Greg. 'The Intelligence Coup of the Century', The Washington Post, 11 February 2020.

Syed, Matthew. *Rebel Ideas*, John Murray: London, 2019.

About the author:

Dr. Robert Dover is Associate Professor of Intelligence and International Security at the University of Leicester, a post he has held since 2016. Before that he was a Senior Lecturer in International Relations, Associate Dean and Institute Director at Loughborough University, and also held fulltime posts at King's College London, and the University of Bristol. He has published widely on governmental usage of intelligence, intelligence practice, foreign policy, and the hybridisation of threats. His latest book on the impact of the digital age on intelligence is due to be published in the winter of 2020.