



University of
St Andrews | FOUNDED |
1413 |



*The Handa Centre for the Study
of Terrorism and Political Violence*

CSTPV Occasional Papers

INTELLIGENCE AND TERRORISM: THE
IMPACT OF TERRORISM ON THE COUNTER-
TERRORISM ROLES AND ARCHITECTURE OF
INTELLIGENCE AGENCIES

D. Chen

INTELLIGENCE AND TERRORISM: THE IMPACT OF TERRORISM ON THE COUNTER-TERRORISM ROLES AND ARCHITECTURE OF INTELLIGENCE AGENCIES

Abstract

Counter-terrorism (CT) has since 9/11 become a leading component of intelligence work, alongside mainstays like political analysis and counterintelligence. The emergence of the Islamic State in Iraq and Syria (ISIS) and new dimensions like extreme right wing (XRW) threats are placing heavy demands on intelligence. This paper addresses three questions. Firstly, whether and how intelligence agencies perform CT roles that go beyond disseminating information. Secondly, whether and how intelligence agencies are involved in CT policymaking. Thirdly, how countries have adapted their intelligence architectures for CT. The research comprised four interviews with senior practitioners and academics, alongside literature surveys. The research focused on the UK, US, Germany and France. Organisational theory was used to frame the analysis as existing intelligence theories were inadequate. The findings showed that intelligence agencies do play CT roles beyond providing information. They include investigating and neutralising terrorists, negotiating hostage releases, discreetly engaging foreign countries on CT, and collaborating with the private sector to build CT capability. However, intelligence agencies are reluctant to engage in CT policymaking out of concern that they might lose credibility if their reporting is politicised or a policy they back fails. The research on intelligence architecture showed that the US's reforms, which were the most sweeping of the countries analysed, were in response to environmental pressures post-9/11 and increased the level of bureaucracy in the intelligence community (IC). The UK's reforms were reactive but less extensive than the US's, while Germany's reforms were proactively initiated and aimed at bolstering CT coordination. The research highlighted that the key environmental influences on CT intelligence work going forward include technology, resource constraints and the legal environment. Day-to-day, intelligence agencies will continue to grapple with issues like how analytical practices can be bolstered to mitigate the risk of politicisation. More research is needed to develop new theoretical frameworks on CT intelligence, update perspectives on the intelligence-policy relationship, and explore applying organisational theory to intelligence work.

Introduction

Just as interest in intelligence started to wane after the Cold War, 9/11 refocused attention on the field. The 2003 Iraq invasion then pushed the issue of intelligence politicisation into the spotlight. In the early 2010s, with al-Qaeda (AQ)'s capability crippled and jihadist violence receding, intelligence debates turned to topics like surveillance and overreach, fuelled by the Snowden and Manning leaks. But ISIS's emergence and the high-signature ISIS-inspired attacks globally since 2014 renewed attention on CT intelligence.

The paper addresses three questions.

- i. Whether intelligence agencies in democracies perform CT roles that go beyond disseminating information to consumers, and if so what they are.
- ii. Whether intelligence agencies are involved in policymaking for CT, and if so what the nature of their involvement is.
- iii. How ICs have adapted their architectures in response to CT demands, and what the considerations driving reforms are.

This paper is timely. Research on the role of intelligence on CT, the intelligence-policy relationship and CT intelligence reforms has tailed off since the late 2000s, prior to which there was intense research on these issues after 9/11 and the Iraq invasion. The role of intelligence beyond providing information remains keenly debated. A focus of the 2016 Chilcot report on the UK's involvement in Iraq was the appropriateness of the IC's involvement in roles beyond the traditional boundaries of intelligence, like involvement in policymaking. The intelligence-policymaker relationship is becoming more dynamic, with ICs having to deal with constant political flux and unfamiliar faces being elected, alongside hot-button issues that can spark political crises if misjudged. ICs are meanwhile facing major shifts in their operating environment, like the growing role of technology in intelligence. Against this backdrop, the terrorist threat remains acute and is assuming new dimensions. ISIS's defeat as a territory-holding group has devolved the ISIS threat to entities like returnees and ISIS-inspired autonomous actors. The West is simultaneously grappling with the growing threat from XRW extremism. Academia is only starting to address these issues in depth.

Summarised findings

For the first question on the CT roles of intelligence, the findings confirmed that ICs fulfil roles beyond disseminating information. The US and France empower intelligence to use lethal force to assassinate terrorists. ICs' other CT roles include responding to terrorist incidents, like tracking down perpetrators or negotiating hostage releases. ICs also front collaborations with the private sector to develop CT capability. But ICs appear reluctant to participate in counter-ideology efforts on the ground.

For the second question, the research indicated that ICs are reluctant to engage in CT policymaking. The fallout over Iraq remains in ICs' minds. In the US and France, distrust between political leaders and ICs perpetuates conditions where policymakers are unlikely to turn to the IC for policymaking advice. The UK and German ICs firmly maintain their distance from policymaking as part of their professional ethos. The findings nonetheless stressed the importance of close intelligence-policymaker coordination, anchored by a robust system to prioritise requirements.

For the third question on how CT has led to intelligence architecture changes, the findings showed that the nature of reforms implemented has varied across countries. Some reforms, like the US's, have been sweeping and increased the level of bureaucracy in the IC, while other countries' have been less extensive. Architecture changes can be categorised as proactive initiatives or knee-jerk reactions to environmental factors. The US's and UK's CT reforms were largely reactions to 9/11 and Iraq, but Germany's reforms have generally been proactively initiated before major terrorist incidents.

Outline

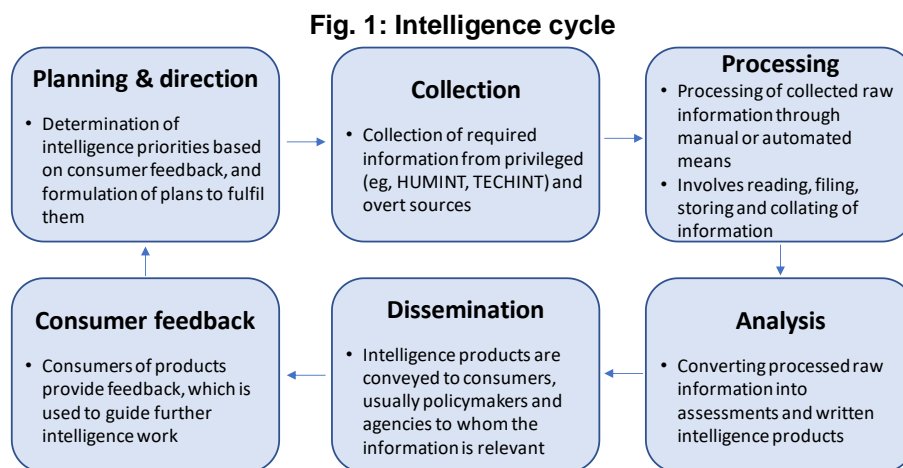
The paper starts with a literature review, which begins by defining intelligence work and discussing the challenges of applying theory to the research. It then outlines the perspectives on the intelligence-policy relationship. This is followed by a survey of the challenges posed to intelligence by CT. The literature review concludes by explaining how this paper contributes to intelligence studies.

The literature review is followed by a short section outlining the methodology of the study. This segues into the analysis component comprising three sections, each addressing one research question. The discussion offers insights arising from the research findings, and discusses them with reference to the present threat environment. It then identifies longer-term CT challenges highlighted by the findings. The conclusion summarises the findings and suggests avenues for future research.

Literature Review

Intelligence cycle and consumers

The components of intelligence work are laid out in the intelligence cycle. (Fig. 1.) The cycle starts with prioritising issues to cover, on which intelligence collects covertly and overtly. Collected data is processed and analysed to produce intelligence products. Products are disseminated to relevant consumers, namely political leaders, bureaucrats, and operational agencies. Products range from complex longer-term strategic assessments to brief tactical “early warning” reports. The cycle is completed when consumers provide feedback on products and the issues to cover.



Good intelligence must be timely, relevant and accurate, in order to be actionable. Reporting should be objective and free from political interference.¹ The value of intelligence is assessed largely by its impact on and usefulness to consumers. For CT, impactful intelligence might prevent an attack, by being accurate and timely enough to enable preventive action.² At the strategic level, impactful intelligence assessments help consumers in policymaking and diplomacy. This can be through accurately assessing counterparts’ moves, providing insights on risks and trends, and discussing scenarios and trajectories.³ In doing so, intelligence gives policymakers what former US Director of National Intelligence (DNI) Mike McConnell called “decision

advantage”.⁴ Sherman Kent noted that intelligence allows consumers to educate themselves, improve policies, and base actions on it.⁵

Consumers, particularly political leaders, play key roles in ensuring intelligence performs optimally.⁶ Policymakers determine what intelligence agencies prioritise and cover.⁷ To provide effective direction, policymakers first need to know how to use intelligence.⁸ For instance, when receiving early warning of an attack, policymakers need to act fast to direct follow-up before opportunities for interdiction are lost. Policymakers need to weigh intelligence alongside other information sources like government agencies or the press. Ideal consumers provide timely and clear direction to the IC, and have a sufficient appreciation of intelligence to adeptly factor it into their decision-making. Some policymakers are even information sources, like diplomats who have interacted with foreign officials who are intelligence targets.⁹

Theory remains underdeveloped

I first attempted to adopt theoretical frameworks from intelligence studies for the research but found them to be insufficient. While the paper focuses on the role of intelligence in CT and intelligence reforms for CT, most intelligence theory remains fixated on explaining traditional intelligence roles like analysis, and has not caught up with current debates. Peter Gill recently said that the intelligence discipline had “spent little time on theorising”.¹⁰ More recent examples of typical work on intelligence theory are the 2012 articles by Richard Betts and Michael Warner. Betts addressed the familiar theme of intelligence failure, while Warner discussed how intelligence mitigates risk.¹¹ Practitioners remain reliant on decades-old frameworks that mostly describe intelligence work, like Kent’s framework for separating intelligence into the elements of knowledge, process and organisation.¹²

Little innovation in the form of novel frameworks has emerged of late. Most intelligence researchers still appear mired in proposing directions for further work, without offering new theories. Loch Johnson’s 2012 article proposed 39 questions for theoretical exploration, without much further elaboration.¹³ Others have just started re-examining established frameworks. Among them, Gregory Treverton in 2018 proposed that for more robust and responsive analysis, ICs should shift away from the intelligence cycle’s linear approach, to an “activity-based” approach where all parts of the intelligence system run concurrently, and both overt and covert information is equally weighted for analysis. Treverton claimed this approach was instrumental in uncovering Osama bin Laden’s location.¹⁴ Mark Phythian notes that more theory is needed on the intelligence-policy relationship to move it beyond familiar concepts like “politicisation”.¹⁵

There are nascent attempts to apply organisational theory to intelligence studies. They include Glenn Hastedt, who sees ICs as “open-facing problem-solving” systems that work on three principles: (i) organise internal activities to achieve outcomes, (ii) enforce boundaries around the organisation to protect intelligence processes from intervention or disruption, and (iii) implement performance assessment.¹⁶ Hastedt co-authored with B. Douglas Skelley an insightful piece on how concepts like bureaucratic theory and environmental theory influence intelligence reforms. Separately, Donald Kettl examined the role of values in intelligence, arguing that the personal values of

the IC and consumer influence what information is disseminated and how consumers use it.¹⁷

Intelligence-policy relationship

Discussions on the intelligence-policy relationship still need to consider the Iraq issue, the fallout over which continues to be studied. It remains an example of how a mismanaged intelligence-policy relationship can lead to politicisation, where the invasion was justified by unreliable intelligence asserting Saddam Hussein's purported possession of WMDs and AQ links.

The "traditionalist" view is that intelligence should be separated from policymaking. This is also referred to as the "Kent doctrine," after Kent who argued for it in 1949. Kent viewed intelligence-policy separation as necessary to ensure analytical objectivity amidst political flux.¹⁸ This view remains popular among ICs, whose officers often pride themselves in staying above the fray. Hans Heymann calls this view a "catechism" that intelligence practitioners take as "hallowed". Intelligence officers view their work as "objective" and "dispassionate", and distinct from "slanted", "adulterated", and "politicised" policymaking.¹⁹

A criticism of the traditionalist view is that too much intelligence-policy separation prevents intelligence from exploiting its subject-matter expertise in policy formulation. Critics believe intelligence agencies should use their expertise to shape policy outcomes.²⁰ This may be through policy advocacy and advice. In reviewing Kent's work, Willmoore Kendall disagreed with Kent's insistence on intelligence-policy separation. Kendall opined that as content experts, ICs should help in policymaking and "influence" outcomes. Kendall felt intelligence-policy separation was "self-defeating" in forcing ICs to desist from contributing their relevant capabilities.²¹

The intelligence-policy relationship is under constant tension²². Both sides are driven by different incentives. While the IC is mostly judged on its reporting, politicians have a gamut of concerns. They formulate policy, canvass support and pay the price should policies fail.²³ Policymakers thus think they incur a higher cost than the IC if there is an intelligence failure.²⁴ The relationship is fundamentally imbalanced, with politicians wielding more influence than the IC that reports to them.²⁵ IC chiefs who are political appointees might instinctively hesitate to rebuff policymakers' requests.²⁶ This may range from minor requests like sharing intelligence with more consumers or for policymakers to read raw intelligence reports, to direct requests for policy support.

Other factors complicating the relationship are the complexity of intelligence work, variety of stakeholders, and emergence of new politicians lacking sufficient understanding of intelligence. New political masters with no experience in intelligence may discard useful intelligence, or fail to effectively direct the IC. This can create intelligence gaps and failures, which for CT means attacks might get through.²⁷ The personalities and worldviews of policymakers also affect the tenor of intelligence-policy collaboration. Some policymakers cannot fathom why intelligence only disseminates information without telling them what to do. Such policymakers, like former US President Richard Nixon²⁸, perceive intelligence as "expand[ing], rather than reduc[ing]" the uncertainty they face, or even "out to get them" by issuing assessments

they disagree with.²⁹ ICs consequently feel aggrieved over policymakers who lack the appetite to digest intelligence products, but still blame the IC for policy failures.³⁰

Despite differing views on intelligence-policy separation, there is consensus that complete separation of intelligence from policy is deleterious. This may lead to both sides becoming uncoordinated, and the IC producing irrelevant products. Kent himself said the danger of intelligence being too disengaged from policy outweighed that of drawing too close.³¹ Eric Rosenbach said that without policy backing, intelligence has no value.³² Betts sees the analysis and policymaking processes as being tightly linked, with policymakers giving feedback on intelligence, which in turn influences policy through its reporting. Because of this, a “complete quarantine” of intelligence from policy is counterproductive.³³

The crux lies in balancing the intelligence-policy relationship. Kent’s view was that intelligence should be close enough to policy to receive maximum guidance, but not lose objectivity.³⁴ The Butler report stressed that the Iraq issue should not distract from the need for “continuity of shared purpose” between intelligence and policy.³⁵ Percy Cradock’s analogy remains popular. He likened the ideal intelligence-policy relationship to “separate but adjoining rooms” in “cheap hotels”, with “communicating doors and thin partition walls”.³⁶ Robert Gates as Director of Central Intelligence (DCI, 1991-93) said the IC should be “right next to the policymaker” to appreciate the policymaker’s agenda.³⁷

Maintaining the intelligence-policy balance is an iterative process. Uri Bar-Joseph called the relationship an “ongoing obstacle race” where both parties bicker.³⁸ This is exacerbated if political changes are frequent. The US IC’s primary challenge with each new administration is adapting to the incoming president and if required educating him on intelligence work. This is essential to laying the desired foundations and boundaries of the IC’s relationship with the new administration, which mitigates the risk of the IC being inadvertently entangled into policymaking during the term. How the intelligence-policy balance is struck affects the quality of the intelligence output. According to the “proximity hypothesis”, greater separation produces assessments that are less biased but possibly less relevant.³⁹ Narrowing the gap leads to more timely, pertinent and influential reporting. In his later writings, Kent stressed that despite the need for intelligence-policy separation, both sides had to maintain open communications for warning-type analysis, like CT.⁴⁰

Risk of politicisation

The starkest risk of involving intelligence in policymaking is politicisation. Politicisation occurs when intelligence reporting is no longer solely focused on facts and unbiased assessments, but is adjusted for political purposes like supporting a policy stance.⁴¹ The analysis becomes biased and distorted.⁴²

Politicisation occurs through various pathways. Top-down politicisation occurs when policymakers exert pressure on the IC. Hastedt categorises top-down tactics into “hard” and “soft” tactics. Hard tactics include policymakers explicitly asking intelligence for a particular line, influencing the intelligence process by appointing pliable IC leaders, or even creating new agencies under their influence. Post-9/11, top US policymakers including the White House and vice-president pressured the IC to link

Saddam to terrorism. In 2002, the Bush administration asked for an intelligence estimate to justify the Iraq invasion. The US defence department meanwhile established an office, which was later disbanded, that disseminated reports emphasising the Saddam-AQ link, when other intelligence agencies were voicing doubt on the purported link.⁴³ Soft tactics include policymakers guiding the intelligence debate in a particular direction, possibly by repeating questions or seeking re-evaluations of an issue.⁴⁴ Bush repeatedly asked the IC to restate its assessments on Iraq and kept calling for the same questions to be answered.⁴⁵ Policymakers can also ignore, or misrepresent in other settings, intelligence reporting that contradicts their plans.⁴⁶

ICs can themselves initiate bottom-up politicisation. This usually revolves around supporting specific policies to garner policymakers' appreciation.⁴⁷ ICs can do so by politicising reporting through various means. They include adhering to a "house line" consistent with policymakers', suppressing dissenting views, offering a range of assessments in reports for policymakers to "cherry pick" their favourite⁴⁸, "sugarcoating" undesirable messages⁴⁹, or omitting information the policymaker would rather not know.⁵⁰ These tactics were on show across the US IC leading up to the Iraq war.⁵¹

The risk for ICs in stepping too far into policymaking is damage to their credibility. This may happen if intelligence supports a failed or controversial policy,⁵² particularly if it is high-signature and politically charged, like involving intelligence in public engagement for counter-ideology efforts. Such engagements can be lightning rods for criticism, and yield curveballs due to the sensitivities involved. ICs that focus on servicing and forging ties with one administration may quickly lose relevance and credibility, if the administration is replaced by one that distrusts the IC because of its perceived allegiances to the old regime.

Intelligence's CT roles

CT places specific demands on intelligence. Its primary deliverable is preventing attacks. ICs face an increasingly challenging operating environment. Challenges include the proliferation of rudimentary plots by self-starters that are difficult to interdict, terrorists' cyberspace use, and the growing XRW threat. CT demands are often more urgent and require quicker policy and covert action, compared to geopolitical analysis. Hastedt observes that some types of intelligence work like CT deal with crises more frequently and run on accelerated timelines.⁵³ Kent said that issuing warnings, which applies to CT, might be more demanding than political assessment, because ICs need to ensure they do not issue inaccurate warnings which might desensitise policymakers to actual threats.⁵⁴

CT generates considerable demands for ICs beyond the intelligence cycle. Some agencies take covert action like assassinating terrorists. Intelligence is also tasked to detect and investigate threat actors, besides passively collecting and reporting on them. CT investigations involve new capabilities like social media intelligence (SOCMINT), where intelligence officers engage suspects online to collect on them and find avenues for interdiction.⁵⁵ CT naturally demands close collaboration with policymakers, perhaps more so than geopolitical analysis. These views were echoed by Arthur Hulnick who said that for CT, ICs should consider closer links with policy.⁵⁶

Kent argued that for the “warning analysis” category like CT, the intelligence-policy distance might have to be reduced compared to political analysis.⁵⁷ CT demands already routinely see intelligence and policymakers working together in task forces or operational units.⁵⁸ CT collaboration is now also a common feature on foreign policy agendas and bilateral accounts, which requires further intelligence-policy coordination.

One by-product of the urgency of CT is that it incentivises intelligence and policymakers to remain in sync and avoid bickering, as both share an interest in preventing attacks. Effective intelligence-policy collaboration will reap rewards. The 2007 troop surge which stemmed the spiralling violence in Iraq was made possible by the IC’s understanding of the threat, coupled with its success in convincing policymakers to approve the surge. But whether intelligence should engage in CT policymaking remains contentious, as CT intelligence is not immune to politicisation and manipulation.⁵⁹

Concluding remarks

This paper contributes to the debate on the CT roles of intelligence. This is relevant amidst the evolving threat landscape, which may compel intelligence to take on more CT roles. The examination of the intelligence-policy relationship for CT is timely, given the renewed attention on the issue following the Chilcot report and strained ties between President Donald Trump and the US IC. The analysis of intelligence reforms for CT demonstrates the unexplored potential of applying organisational theory to studies on intelligence management.

Methodology

A qualitative study was conducted, combining literature research and interviews. For each research question, theoretical frameworks were used to formulate a hypothesis. The hypotheses were tested against findings from literature research and interviews. The research focused on the UK, US, Germany and France, as they are democracies with established ICs. Examples from other countries were provided where relevant. The literature research covered journals, books, government reports and policy documents.

Four interviews were conducted, with

- i. David Omand (13 Mar 19, London). Omand was GCHQ director (1996-97), Home Office Permanent Secretary (1997-2000) and UK Security and Intelligence Coordinator (2002-05).
- ii. Peter Jackson (21 Mar 19, Glasgow), Glasgow University chair in Global Security.
- iii. Jonathan Evans (16 Apr 19, St Andrews), MI5 director-general (2007-13).
- iv. Xavier Raufer (19 Jun 19, Paris), director of the Department for the Study of Contemporary Criminal Menace at the Paris Institute of Criminology.

The interviews were semi-structured. They were guided by broad questions, but interviewees were invited to comment on any issues they thought relevant. The interviews were face-to-face.

Besides research on the CT roles and architectures of ICs which are directly relevant to the research questions, further research on the threat situation in Europe and North America was done to ground the analysis in a real-world context.

Theoretical frameworks

A combination of intelligence concepts and organisational theory provided the theoretical frameworks for analysis. The intelligence frameworks referenced include the intelligence cycle, the “Kent doctrine” favouring intelligence-policymaking separation, and frames on the mechanism of intelligence politicisation. But existing intelligence theories could not adequately provide an analytical framework, because the research questions were novel. Available theories were largely focused on traditional intelligence roles like analysis, while the emphasis of the study was on the mandate and management of CT intelligence. Because of this, organisational theory was used to formulate the required analytical frameworks.

For the first question on ICs’ CT roles, McKinsey’s and Bain’s frameworks for evaluating business expansion, alongside SWOT⁶⁰ and TOWS⁶¹ matrix derivations, were used to identify types of strategies ICs might explore for CT. These strategies were overlaid onto a spectrum of CT roles, to build a landscape map showing where ICs might have additional CT roles. For the second question on whether ICs are involved in CT policymaking, a cost-benefit approach was used to argue that ICs should not do so. This argument was used to abductively arrive at the hypothesis that ICs are unlikely to engage in policymaking as the risks and costs outweigh the benefits. For the third question on how CT demands have shaped intelligence architecture, bureaucratic and environmental theories were used to examine recent reforms. The Capstone change model was used to evaluate and classify reforms, according to their extensiveness, and whether the changes were proactively or reactively initiated.

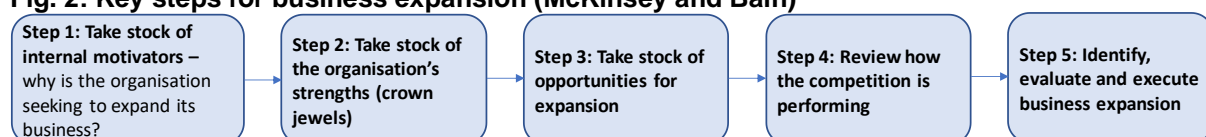
Research Question 1: Role of Intelligence in CT

This section examines if and how intelligence agencies perform CT roles beyond disseminating information. It tests the hypothesis that ICs go beyond providing information, in synergistic areas closely related to intelligence agencies’ natural strengths.

Theoretical framework

I approached this issue with theories by McKinsey and Bain on how organisations assess business expansion opportunities.⁶² Both McKinsey’s and Bain’s theories on business expansion have the same key stages, outlined in Fig. 2. Both advise that expansion strategies leverage on existing strengths, and that expansion areas should not stray far from the core business.

Fig. 2: Key steps for business expansion (McKinsey and Bain)



SWOT and TOWS analysis is well-suited to identifying and evaluating industry gaps for expansion, which is a key focus of McKinsey’s and Bain’s frameworks. SWOT identifies an organisation’s internal strengths and weaknesses, alongside external opportunities and threats, which correlates to steps 2-4 of the process in Fig. 2. SWOT findings are used to derive the TOWS matrix which surfaces four strategy approaches for consideration, shown in Fig. 3.

Fig. 3: TOWS matrix

		External factors	
		Opportunities	Threats
Internal factors	Strengths	Maxi-maxi strategies: Use strengths to maximise opportunities	Maxi-mini strategies: Use strengths to minimise threats
	Weaknesses	Mini-maxi strategies: Minimise weaknesses by exploiting opportunities	Mini-mini strategies: Minimise weaknesses and avoid threats

I worked off the SWOT and TOWS findings to derive a landscape map, to identify theoretical gaps in the CT landscape where ICs might have roles. (See following paras and Fig. 5.)

Hypothesis

SWOT analysis helped identify the inherent strengths and weaknesses of intelligence agencies for CT, along with possible external opportunities and threats. (Fig. 4a.)

Fig. 4a: SWOT exercise for intelligence agencies for CT

Internal factors	Strengths 1. Covert collection mandate 2. Covert action mandate 3. Deep subject matter expertise not found elsewhere in government 4. Ability to keep a low profile in external dealings	Weaknesses 1. Barriers to information flow due to operational security considerations 2. Risk of infighting (especially in complex intelligence ecosystems) 3. Risk of groupthink in analysis
External factors	Opportunities 1. Gaps in CT landscape not adequately fulfilled by other agencies 2. CT areas where ICs can do better or add significant value , even if other agencies are addressing them	Threats 1. Credibility risk to ICs , eg, due to intelligence failure or a botched covert action that is revealed 2. Security risk from intelligence being compromised , eg, due to espionage

A TOWS matrix was derived from the SWOT components. (Fig. 4b.) TOWS indicates that analysis on how ICs might grow their CT roles should be focused on the maxi-maxi quadrant. The other three quadrants are less relevant. This is because in intelligence, “weaknesses” and “threats” like information barriers, groupthink or credibility risks are primarily addressed through policy and process modification. For instance, removing information barriers by broadening access to intelligence (addressing a weakness) entails accepting more security risk (exacerbating a threat), which is a policy call.

Fig. 4b: TOWS matrix for CT intelligence work

		External factors	
		Opportunities	Threats
Internal factors	Strengths	<p>Maxi-maxi strategies: Use strengths to maximise opportunities</p> <p><i>Leverage on core strengths of covert collection, covert action, subject-matter expertise and ability to keep a low profile, to fill CT gaps or value-add in specific CT areas where intelligence is well-placed to do so</i></p>	<p>Maxi-mini strategies: Use strengths to minimise threats</p> <p><i>Less relevant in intelligence context. Threats to intelligence work (eg, loss of credibility arising from failure), should be addressed through policy and process</i></p>
	Weaknesses	<p>Mini-maxi strategies: Minimise weaknesses by exploiting opportunities</p> <p><i>Less relevant in intelligence context. Weaknesses in intelligence work (eg, stovepipes, groupthink), should be addressed through policy and process</i></p>	<p>Mini-mini strategies: Minimise weaknesses and avoid threats</p> <p><i>Less relevant in intelligence context. Weaknesses and threats should be addressed through policy and process</i></p>

To arrive at the hypothesis that ICs are fulfilling additional CT roles that build on intelligence agencies' strengths, the maxi-maxi quadrant was expanded into a landscape map (Fig. 5) to identify additional areas where ICs might contribute. This involved mapping the spectrum of CT tasks against ICs' strengths and opportunities. The deliverables from the UK's CONTEST strategy were extracted to illustrate the spectrum of CT work, as CONTEST is a comprehensive whole-of-government CT plan. Some additional CT tasks not included in CONTEST were also included.

Fig. 5: CT landscape map for identifying additional areas for intelligence to contribute
 (Blue boxes denote additional roles where ICs may contribute)

		Internal STRENGTHS of intelligence agencies				External CT OPPORTUNITIES			
		Covert collection	Covert action	Deep subject-matter expertise	IC's ability to keep a low profile	Currently not or inadequately fulfilled by govt (UK context)	IC can add value or do better		
Spectrum of CT tasks (extracted from CONTEST)	Prevent strand of CONTEST	Tackle root causes of radicalisation			Possible		Yes	Possible (eg, to analyse trends, but not actual engagement)	
		Intervene in those at risk	No intel role						
		Rehabilitation	No intel role						
		Prevent online dissemination of extremist material	Yes	Possible, eg, takedowns	Yes				Yes
		Community partnerships	No intel role						
		Safeguard vulnerable groups, eg those with mental health issues	No intel role						
		Prevent radicalisation in educational settings	No intel role						
	Share intel with greater range of partners							UK IC is looking into sharing intel more widely with relevant consumers	
	Pursue	Understand, detect and investigate terrorism	Yes		Yes				Already core intel work
		Disrupt terrorism (including covert action), including overseas	Yes	Yes	Yes				Already core intel work
		Prosecute terrorists							
		Introduce CT legislation							IC's input already being sought on CT laws
		Manage, pool and share terrorism data							IC already involved in effort
		Address foreign fighters	Yes		Yes				IC already involved in effort
		Address terrorist financing	Yes		Yes				IC already involved in effort
		Independent oversight of CT, including by independent reviewer of CT legislation							Independent reviewer works closely with IC
		Encourage citizens to proactively watch for terrorist activity							N.A. for intel
		Engage private sector in investigation and analysis				Yes	Yes		More intel-private collaborations can be explored
	Address returnees	Yes	Yes	Yes	Yes			Already being addressed by intel	
	Protect	Disseminate strategic CT reads to inform policy*	Yes		Yes				Already core intel work
		Disseminate tactical threat assessments to enable action by operational agencies*	Yes		Yes				Already core intel work
		Deal with terrorists at the border	Yes		Yes				Already core intel work
		Protect critical infrastructure	Yes		Yes				Already core intel work
		Protect crowds, vulnerable groups, VIPs	Yes		Yes				Already core intel work
		Address insider threats	Yes		Yes				Already core intel work
		Prevent access to attack materials and expertise							
		Enhance CBRN capability							
	Prepare	Coordinate multiagency response to attacks							
		Minimise attack impact	No intel role						
		Bolster emergency services	No intel role						
Support victims		No intel role							
Return attack site to normal use		No intel role							
Develop response capability to specific types of attack, eg CBRN									
Involve military if necessary									
Negotiations to release hostages*	Yes, to collect on hostage-takers				Yes, to keep negotiation discrete		Yes		
Intelligence diplomacy, eg with foreign govts, following terrorist incidents*					Yes, to keep negotiation discrete		Yes		

* Additional deliverables not mentioned in CONTEST.

The map surfaces several areas beyond collecting and disseminating information where intelligence might contribute.

- i. Covert action, ranging from special operations to kill targets, to takedowns of extremist websites.
- ii. Post-attack response, where ICs' ability to conduct dealings away from public scrutiny is an asset for sensitive negotiations with hostage-takers or foreign governments, which may be jeopardised by public or media attention. Eg,

- discrete negotiations with governments may be needed if attackers are foreign and make demands of their governments like the release of detainees.
- iii. Private-sector collaborations with government to build CT capability, where especially sensitive collaborations on areas like surveillance can be kept away from public view by ICs' ability to conduct business discretely.
 - iv. Counter-ideology, where various governments have acknowledged more needs to be done. Intelligence agencies may have a better understanding than other government departments on related issues like the root causes of radicalisation.

The map thus helps illustrate the hypothesis that intelligence likely has additional CT roles, which are closely related to intelligence agencies' core strengths, beyond collecting and reporting information.

Findings

On covert action, some intelligence agencies are empowered to take lethal action. The CIA's deployment of drone strikes is one example.⁶³ France's Direction Générale de la Sécurité Extérieure (DGSE) maintains a "Groupe Alpha" that has assassinated terrorists dating back at least to the 1990s. Then President Francois Hollande publicly acknowledged in 2017 that DGSE maintained militant hitlists.⁶⁴ But the UK and German ICs do not appear to have the same mandate. Ex-MI6 Chief Richard Dearlove said at an inquest into the death of Princess Diana in 2008 that "assassination is no part of the policy of Her Majesty's Government".⁶⁵ German agencies are legally barred from taking direct tactical action like arresting suspects.

Most intelligence agencies have roles in responding to terrorist incidents. The IC's post-attack role includes detecting perpetrators, investigating leads, and possibly collecting on foreign governments' responses (eg, if the attackers are from their countries).⁶⁶ Developing contingency plans are a priority for ICs, which now often assume that not all attacks can be prevented. Evans notes this places a premium on the post-attack response and pre-emptive measures to mitigate the potential damage of attacks. For instance, in the 2017 London Bridge attack, police arrived in minutes, and casualties were probably limited by the UK's strong firearms restrictions.⁶⁷ Intelligence agencies may be called on during hostage situations. Agencies such as BND (Bundesnachrichtendienst), DGSE and Spain's Centro Nacional de Inteligencia (CNI) front hostage negotiations.⁶⁸ The situation is different in the UK and US where the official policy is not to negotiate with terrorist hostage-takers, even though negotiations have nevertheless occurred in some cases.⁶⁹ The capture of British hostages triggers a multiagency response that involves intelligence agencies, which are tasked to collect relevant information, although there is no public reporting on whether they participate in actual negotiations. The capture of American hostages similarly triggers a multi-agency response, which varies across incidents. During negotiations with the Taleban to free US soldier Bowe Bergdahl in 2014, State Department negotiators were accompanied by CIA agents. The latter facilitated the talks but whether they participated in actual negotiations is unknown.⁷⁰

As suggested by the landscape map, intelligence-industry CT collaboration is a growth area. Then UK Home Secretary Sajid Javid stressed the need for more of such collaboration when launching the updated CONTEST strategy in 2018.⁷¹ The private sector is a valuable source of intelligence. In this vein, MI6 is expanding collaboration

with industry through the National Security Strategic Investment Fund.⁷² The US's National Strategy for CT (2018) similarly emphasised expanding industry collaborations.⁷³ The Snowden leaks spotlighted the US IC's collaborations with Booz Allen Hamilton on surveillance. CIA earlier funded technology startup Palantir, which specialises in data-mining and information processing on entities.⁷⁴

Western ICs appear reluctant to involve themselves in counter-ideology. Intelligence agencies' role here may be limited to disseminating reads on related areas like the root causes of terrorism. But engaging in public outreach for counter-ideology appears to be a no-go area. A key concern for ICs is that counter-ideology initiatives are often politically sensitive, which may result in missteps that incite public criticism, when the role and risk can be devolved to other agencies. Evans noted that in the UK, MI5 has decided against getting involved in community engagement as it might distract from MI5's core work. This was after MI5 explored outreach efforts, like an engagement session with teachers fronted by Evans. Community engagement for counter-ideology has meanwhile fallen to the UK police. The German IC is also not involved in counter-ideology, which is the responsibility of other departments. In France, counter-ideology has been devolved to an array of law enforcement, prison and local authorities.⁷⁵ The US does not have a comprehensive and coordinated counter-ideology strategy. Past counter-ideology efforts were piecemeal and involved agencies other than the IC, such as a State Department-led effort to discredit ISIS's discourse which was panned as ineffective.⁷⁶

Focus remains on core intelligence cycle roles

Although ICs are engaged in a growing range of CT roles, the bread-and-butter work of collecting privileged information and disseminating it remains their preoccupation. Covert collection, coupled with the deep institutional knowledge on CT that ICs bring to bear in their analysis, are "crown jewels" unique to ICs. These tasks remain labour-intensive as technology still cannot significantly cut the effort needed for HUMINT and analysis. Mark Lowenthal notes that while IT is now good at "amassing data", the search for automated analysis tools has not been as fruitful, and that analysis still remains an "intellectual" instead of "mechanical" process.⁷⁷

Even within the collection and reporting roles, CT places additional demands on ICs, above the expectations for other missions like geopolitical analysis. The intelligence cycle for CT typically runs faster than political analysis. Directions to intelligence may be needed in almost real time during an attack.⁷⁸ Another defining feature of CT intelligence is the demand for tactical reporting in addition to strategic assessments. This includes threat assessments (TAs), which in the UK are issued by the Joint Terrorism Analysis Centre (JTAC). Tactical reporting means the intelligence agency needs to serve a myriad of additional tactical/operational-level agencies and departments that consume such reporting. For instance, TAs and tactical CT reports are sent directly to "expert consumers" like Scotland Yard (SO15).⁷⁹

The need to investigate threat actors places additional collection and processing demands on ICs for CT. In the latter, collection is largely limited to tapping cultivated human agents, or passively collecting data through TECHINT. But CT requires ICs to go beyond this to aggressively investigate threat actors once detected. This requires labour-intensive operations, often online, to engage the actor to uncover his networks

and lure him into revealing actionable intelligence. These requirements have given rise to the new field of SOCMINT, which encompasses the harvesting of intelligence and the running of live investigations on targets on social media.⁸⁰

Concluding remarks

The research substantiates the hypothesis that intelligence agencies are playing CT roles beyond the confines of the intelligence cycle, in areas where their core strengths can be leveraged on. This includes utilising their covert action mandate to neutralise terrorists, or their ability to conduct discrete dealings for hostage negotiations or sensitive industry collaborations. Intelligence agencies however keep themselves at arm's length from the politically-sensitive public engagement aspect of counter-ideology. The core intelligence cycle functions of collecting and reporting on threat actors, alongside actively investigating them, will remain the mainstay of CT intelligence work.

Research Question 2: Intelligence-Policy Relationship for CT

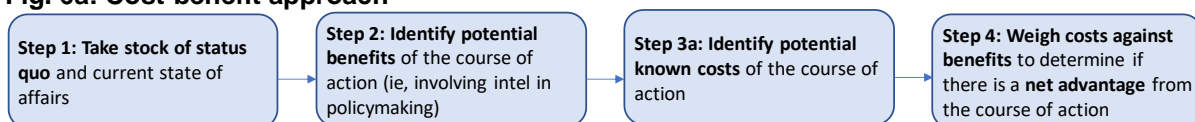
This section further develops the theme of the role of intelligence in CT, by examining whether and how intelligence agencies are involved in CT policymaking. It discusses the motivations of the intelligence and policy communities for either increasing or reducing the distance between intelligence and CT policymaking.

Theoretical framework

While the question addressed whether and how ICs engage in CT policymaking, I approached it abductively by first considering if ICs should do so based on the potential benefit to the IC, before working backwards to hypothesise if they are likely to. This abductive approach is suggested by Gill for studies on intelligence processes, because available theory is thin and many aspects of intelligence cannot be directly observed.⁸¹

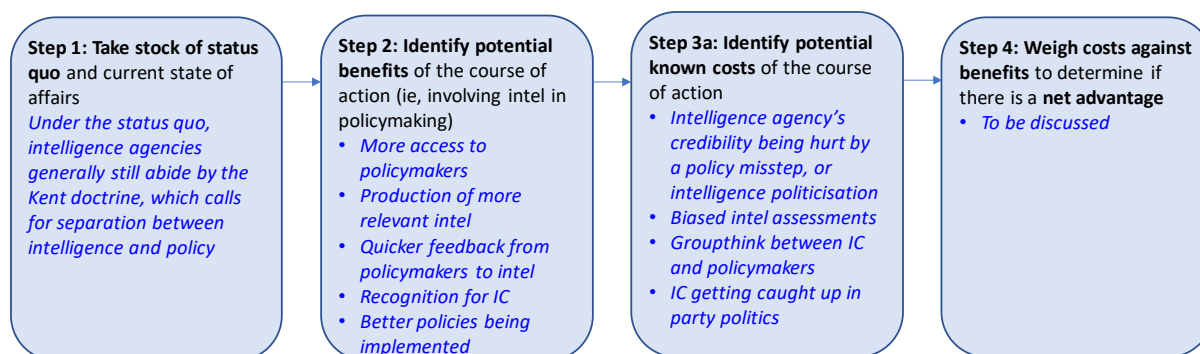
To see if ICs should engage in policymaking based on value, I used a qualitative cost-benefit approach to examine if the costs and risks of involving intelligence in policymaking outweigh the benefits. This approach is adapted from the key steps in a typical cost-benefit analysis of business strategy, with the quantitative component omitted. The basic steps of the cost-benefit approach are shown in Fig. 6a.

Fig. 6a: Cost-benefit approach



Based on existing literature on the intelligence-policy relationship, a qualitative cost-benefit exercise on involving intelligence in policymaking is shown in Fig. 6b.

Fig. 6b: Cost-benefit analysis on involving intelligence in policymaking



The exercise highlights that the tradeoff for involving the IC in policymaking is between the potential for intelligence input to yield better policies, against the credibility risk that ICs shoulder by engaging in policymaking. ICs' deep expertise on CT would allow them to make well-nuanced policy recommendations expeditiously. But the downside is the erosion of ICs' reputation as credible and unbiased voices, if an intelligence-backed policy misfires, or if ICs disseminate politicised intelligence that leads to major intelligence failure. In the CT context, this might occur if an intelligence agency withholds threat reporting out of political considerations, leading to a preventable attack occurring. In fiercely contested political systems, ICs might get embroiled in party politics and face allegations of bias if they engage in advocacy. ICs may decide that there is no critical need for them to advocate policy anyway, as this can be delegated to other government policymaking agencies. Even if they do not have the same level of institutional understanding of CT that intelligence agencies have, entities like home ministries are often able to competently conduct CT policymaking. Any additional utility from intelligence agencies' policy input would thus be marginal. There is therefore a strong argument that ICs should maintain a clear separation from policy work and desist from venturing into policymaking. This is not only to safeguard ICs' neutrality, but also because the value-add of ICs doing policy work is unclear.

Hypothesis

Based on the argument that ICs should not engage in policymaking because the costs outweigh the potential gains, the hypothesis is that ICs in democracies will not be inclined to participate in CT policymaking, over concerns that their reputation and credibility may be hurt by political fallout.

Findings

The research corroborates the hypothesis that ICs are presently reluctant to engage in CT policymaking. The fallout from the politicisation of intelligence to justify the Iraq invasion continues to weigh on Western ICs' minds, particularly the US's and UK's.

In the US, the Kent doctrine in favour of intelligence-policy separation gained renewed popularity after Iraq. Post-invasion, various voices renewed calls for intelligence-policy separation. Former US Middle East National Intelligence Officer (NIO) Paul Pillar wrote in 2006 that the "proper [intelligence-policy] relationship" which "sharply separates" their functions was "upended" in the decision to invade Iraq. Pillar added that ICs should report facts, while avoiding policy judgements and advocacy.⁸² Former US National Intelligence Council (NIC) Chairman Thomas Fingar wrote in 2011 that

intelligence practitioners “don’t do policy”.⁸³ Former FBI Director James Comey said in 2018 that the president and FBI should be kept “at arm’s length”.⁸⁴ Among academics, James Bruce and Roger George said that a cornerstone of intelligence is maintaining “relevance while assiduously avoiding policy advocacy”.⁸⁵ Joshua Rovner wrote that inadequate separation from policy raised the risk of intelligence failure by amplifying existing viewpoints across the intelligence and policy communities, obscuring new threats.⁸⁶

Pragmatically, the extent to which the US IC is involved in policymaking is largely influenced by personal relationships between the president and IC heads, particularly the Director of the CIA (DCIA). To this end, there is little material indicating that the Trump and Obama administrations have habitually turned to the US IC for policy advice or support. Trump’s disdain for the IC means he is unlikely to trust policy advice from the IC.⁸⁷ There is no public evidence either to suggest Obama sought to increase the IC’s involvement in policy while president, even though Obama and the CIA reportedly enjoyed a generally cordial working relationship, during which time Obama acceded to various CIA requests for more CT resources.⁸⁸ For his part, Obama’s 2009 address to the CIA called on the agency to provide more and better intelligence amidst the fluid foreign policy environment. But Obama did not ask CIA to embrace new roles, much less suggest it should be more involved in policy.⁸⁹

Nonetheless, some US IC involvement in policymaking cannot be ruled out. Periodic hints continue to emerge of US intelligence agencies being involved in policy deliberations or still occasionally politicising assessments. For instance, the US’s practice of designating Foreign Terrorist Organisations (FTO) is likely politicised to some extent, even if it is portrayed as intelligence-led. Ex-DNI James Clapper said in 2018 that the US’s initial circumspection about designating the Haqqani Network as an FTO might have been because this would portray Pakistan as a state sponsor of terrorism, at a time when Pakistan was a key US CT partner.⁹⁰ In 2015, a whistleblower revealed that US Central Command (CENTCOM) leaders were disseminating reporting that was more optimistic about progress against ISIS, than what CENTCOM analysts were assessing. CENTCOM leaders’ actions were probably motivated by a desire to have their reporting resonate with Obama’s narrative that ISIS’s defeat was imminent.⁹¹

The UK IC is unequivocal about its principle of not participating in policy. The UK IC has also shown resolve to learning from the Iraq episode, where it may have ventured too far into the policy space. Omand notes that the Kent doctrine remains “alive and well” in the UK.⁹²

A defining feature of the UK IC is the Joint Intelligence Council (JIC), which is responsible for all-source assessment and a unique setup among the countries covered. Unlike other countries whose main external or internal intelligence services do their own analysis, MI6 and MI5 focus on collection, while JIC aggregates all-source intelligence and does analysis. To do so, JIC brings together career intelligence officers and policymakers seconded to the outfit. UK-based observers generally think JIC performs well and should be retained. The Chilcot report reiterated that JIC’s separation of collectors from analysts is a “very important strength” of the UK system.⁹³ Omand identified two advantages of the JIC setup, namely enabling policymakers to

easily contribute any expertise they have to the assessment process, and constantly sensitising policymakers to the IC's latest thinking on an issue.⁹⁴

As a rule, JIC never advises on policy. While JIC is partly staffed by seconded policymakers, they serve as expert consultants and never advocate policy in their JIC capacities.⁹⁵ The Chilcot report reiterated this. Omand told the Chilcot inquiry that the "golden rule" for JIC was that it would "never venture a view on policy even if asked". John Scarlett (JIC chairman during the Iraq invasion) also told the inquiry that "discipline was very strong" on the IC end to maintain separation from policy.⁹⁶

UK IC heads play a key role in holding the intelligence-policy line. They routinely resist occasional requests to step more into the policy space. Omand said there was a "natural temptation" for principals to ask MI6 chiefs for their views on policy, but the latter would decline. Scarlett routinely did so.⁹⁷ A retired senior security official said that some UK IC chiefs deliberately distance themselves from politicians, because they feel staying too close to politicians is improper.⁹⁸

UK policymakers' own averseness to sharing policymaking responsibilities with the IC, coupled with the ringfencing of certain intelligence processes from policymakers, further serves to separate intelligence from policy. Omand surmised that some policymakers like defence secretaries would tell the IC to "get back into the box", if the IC were to ever cross the line and attempt to advocate policy.⁹⁹ At the working level, processes like the issuing of terrorism TAs of the national threat level as well as on individual events or entities, have been delineated as the IC's sole responsibility. This helps discourage political interference, as TAs are a key tool for guiding policy and communications on threats, and the recommendations can be controversial. Evans noted that the TA process is "carefully protected", and that TAs are professional assessments and approved by the JTAC head, while politicians have played their part by not interfering.¹⁰⁰

A key takeaway for the UK IC from Iraq is that while its conduct was generally professional, it occasionally stepped too far into the policymaking space, as when it facilitated the government's efforts to justify the war. Much of the controversy over the UK IC's role on Iraq surrounded JIC's overseeing the compilation of the "September Dossier"¹⁰¹ in 2002. This document was prepared for a parliamentary discussion, and laid out the arguments in favour of the UK's participation in the invasion. JIC's role in the dossier saw the UK IC take the rare step of getting involved in a public debate on a policy decision. This thrust the IC into the highly-charged atmosphere of crisis-period political decision-making.¹⁰² The Chilcot Report concluded that the issue of the dossier underscored the need for "clear separation" between intelligence assessment and policymaking.¹⁰³ Evans reflected that while the dossier was based on intelligence, it was nevertheless influenced by policy to some extent and pushed the boundary of what could be considered an acceptable intelligence product. Evans attributed this to some IC leaders at the time being too closely aligned to politicians, leading to them doing what the ministers wanted.¹⁰⁴ A degree of the politicisation of the intelligence process also came from the top. Then PM Tony Blair inaccurately characterised intelligence reporting to parliament and the public to justify the war, by asserting that intelligence had unambiguously established Saddam's possession of WMDs when the raw data was less conclusive.¹⁰⁵ Blair repeated these assertions in his forward that was attached to the dossier. The Chilcot report noted that in hindsight, JIC should

have highlighted the significant uncertainty in the intelligence being cited by Blair when dealing with him, and done more to restrain him from publicly casting this intelligence in unequivocal terms, such as in his forward.¹⁰⁶ But this is easier said than done, as intelligence chiefs would be understandably reluctant to go against their political masters, especially if they know a policy decision has been made (see next para).

The UK's involvement in Iraq highlights how bilateral relationship considerations can supersede intelligence in policymaking. Evans noted that it was difficult for the UK government to openly articulate its calculations for joining the invasion, which were driven considerably by "Anglo-American relations"¹⁰⁷, namely the UK's historical tendency to stand by the US. By early 2002, even before parliamentary debates in the UK on Iraq commenced, the government viewed an invasion as "inevitable", with Bush bent on removing Saddam and justifying this by linking Saddam's purported WMD programme to terrorism.¹⁰⁸

There are some dissenting voices on the ability of the UK IC and particularly JIC to stay above the political fray. Jackson argues that the intelligence-policy line in the UK is "blurred" precisely because JIC enlists policymakers who serve an intelligence function in JIC while retaining their policymaker hats. Jackson thinks that under these circumstances, it is impractical to expect double-hatting JIC members to fully separate their intelligence and policy roles, which makes the intelligence-policy separation "artificial".¹⁰⁹

In Germany, there is clear separation of intelligence from policy. German law enforces the separation of intelligence from policy and operational action. The Federal Intelligence Services Act stipulates that intelligence agencies have no political authority or law enforcement powers. Similar to JIC's professional discipline in resisting requests from policymakers to comment on policy, German intelligence heads do likewise. German IC heads meet ministers and top bureaucrats for regular security meetings, but refrain from giving policy advice. There may be an ethnolinguistic element to how the German IC views the intelligence-policy relationship. The German word for 'intelligence' – *Nachrichtendienst* – is literally translated as 'news service', which may explain why the German IC perceives itself as mainly a purveyor of facts and little else.

However, intelligence-policy separation in Germany has not prevented the IC from periodically wading into CT-related political controversies. This has happened on XRW issues, where missteps by the Bundesamt für Verfassungsschutz (BfV) have caused consternation. Then BfV President Hans-Georg Maaßen's public denial of obvious evidence of XRW targeting of migrants in 2018 prompted his removal and threatened to destabilise Angela Merkel's government. In 2019, BfV landed in another maelstrom when it was judged to have defamed the far-right Alternative for Germany (AfD) party, by targeting it for investigation for extremism without sufficient evidence.¹¹⁰ In such instances, intelligence cycle processes may not have been compromised or politicised. But the political fallout can still tarnish the IC's standing, strain the intelligence-policymaker relationship, or portray the IC as biased.

In France, the intelligence and policy worlds do not mix for cultural reasons. According to Raufer, politicians and top bureaucrats from prestigious ministries like the defence and foreign ministries look down on and distrust the IC. Policymakers are thus not

inclined to turn to the IC for policy advice, even though the IC is highly competent on CT. Raufer explained that the ill-will between the political elite and French IC is deep-seated and has elements of classism. The former generally hail from elite families around Paris, but the IC's ranks are dominated by those of middle-class background from across the country. French politicians thus rather lean on other quarters for political manoeuvring and support, such as journalists, who usually come from similarly privileged backgrounds.¹¹¹

Comments

The practitioners interviewed echoed the academic community's caution against putting too much distance between intelligence and policy. They agreed that close coordination between intelligence and policy is vital for CT success. Evans said that while the intelligence and policy roles are clearly defined, their work processes are not entirely separate. Because of this, both sides "do not and should not stay at arm's length", and it would be "silly" to put more distance between them. To illustrate the tight intelligence-policy loop, Evans said that JIC provides intelligence briefings at National Security Council (NSC) meetings, while intelligence heads regularly meet supervising ministers and attend permanent secretary-level "Sherpa" meetings where policy issues are discussed. Evans added that on some policy areas like what CT laws the IC needs, it would be "odd" if the IC cannot weigh in.¹¹² Omand wrote that while the IC and policymakers should not get too "comfortable", "real life requires a balanced relationship". To this end, JIC ensures both sides are "geared actively" and can "react on" each other, so each has buy-in on recommendations and assessments made.¹¹³ A coordinated intelligence-policy relationship pays CT dividends. This is probably a key reason behind the UK's success in disrupting many times more plots than there have been successful attacks.

Having an effective system for the IC and policymakers to discuss and agree on intelligence priorities is crucial to the proper functioning of the intelligence-policy relationship. Ruben Arcos and Jose-Miguel Palacios note that to work well, intelligence agencies need a keen awareness of consumers' preoccupations to strategise how they can be fulfilled by intelligence, which broadly describes the priorities process.¹¹⁴ The priorities-setting process helps ICs stay in sync with policymakers' priorities, which ensures the IC's reporting is relevant. This is important in CT, where fast-moving developments can mean sudden changes to priorities. In the UK, the IC works with JIC to propose a priorities list which the political leadership approves.¹¹⁵ In Germany, BND maintains a priorities "mission statement" (Auftragsprofil-der-Bundesregierung), which is updated when needed. Updates may be decided at coordination meetings between the IC and policymakers. The priorities-setting system does not appear to run well in France. Raufer lamented that the testy relationship between French intelligence and policymakers means the government often sends taskings too late for the IC to deliver to its potential.¹¹⁶

Another takeaway from the Iraq episode is that intelligence agencies should proceed cautiously with public engagement to garner support for a policy. This could open the IC to disruptive criticism over the policy. The risks to the IC would be higher if the proposed policy or action is controversial or based on questionable intelligence, such as the decision to invade Iraq. With regard to the September Dossier which was used for similar purposes, the Chilcot report concluded that publicising JIC's role in it was a

misstep that resulted in more weight being placed on the reporting than could be justified¹¹⁷. Daniel Lomas and Christopher Murphy said that JIC's statements in the dossier were no longer "unbiased assessments" but a public relations exercise, which thrust JIC into "public controversy with long-term implications".¹¹⁸ In the US, the epitome of the use of intelligence for public relations was then Secretary of State Colin Powell's televised UN briefing to justify the Iraq invasion, with then DCI George Tenet seated immediately posterior for visual impact. Pillar has also written at length on ICs' involvement in public relations. He described Powell's performance as a deviation from the "professional standard" by using policy to drive intelligence, instead of the expectation for an unbiased IC to convey unvarnished intelligence to policymakers. Pillar added that this showed how the Bush administration cherry-picked raw reporting regardless of its reliability to substantiate the Saddam-AQ link. Pillar then said that on the public relations front, the US should emulate the UK, which after the Iraq episode publicly declared that the IC should not advocate policies still being debated.¹¹⁹

ICs might not have a choice about stepping into the public debate. They can get dragged into the fray by policymakers who call for intelligence to back or advocate policy. The US IC was pushed into policy advocacy on Iraq¹²⁰, even though it internally disagreed with senior administration members' stance that Saddam was complicit with AQ.¹²¹ ICs can partially protect themselves when they cannot avoid public engagement. The Chilcot report suggested that whenever intelligence is used for public debate, intelligence assessments must be clearly delineated from advocacy. The report also advised more independent scrutiny of any intelligence used for such purposes.¹²² That said, the UK has continued to publicise selected IC work to raise awareness of the IC's CT efforts, such as the report on the 2017 London and Manchester attacks by Independent Reviewer of UK Terrorism Legislation David Anderson.¹²³

Concluding remarks

The research corroborates the hypothesis that ICs are keen to avoid getting involved in policymaking. The US's and UK's approaches on the intelligence-policy relationship have been influenced by the Iraq invasion, with both countries launching concerted efforts to alleviate the risk of future intelligence politicisation. Distrust between Trump and the US IC, and between French politicians and their IC, currently discourages their intelligence and policymakers from drawing too close. In the UK and Germany, strict intelligence-policy separation is maintained by a combination of appropriate structures, work processes and professional culture. The research underscores the importance of having a system for ICs to negotiate intelligence priorities with consumers, and the risks of enlisting ICs in public relations efforts for policy support.

Research Question 3: Influence of Counter-terrorism on Intelligence Architecture

This section studies how countries have adapted their intelligence architectures for CT. Various countries have tweaked their CT architectures since 9/11, ranging from fundamental changes in the US to less sweeping refinements and tweaks elsewhere. Studies of the impact of these changes have only recently gained momentum. I used organisational theory for this analysis, because as Hastedt and Skelley note,

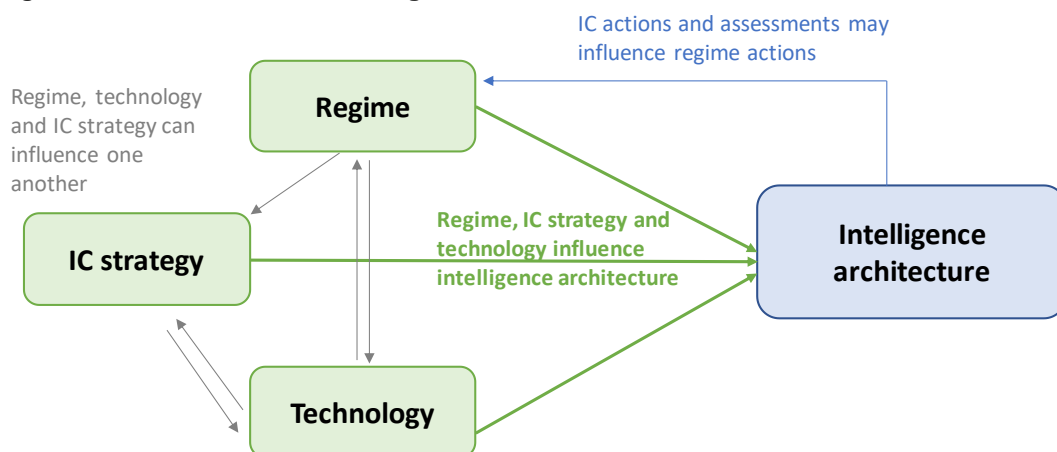
assessments of intelligence reform will benefit by being rooted in such literature, but most studies have not done so.¹²⁴

Theoretical framework

The bureaucratic and environmental theories are relevant to this question on intelligence architecture. Bureaucratic theory argues that organisations boost efficiency by making structural changes to clarify roles, better structure decision-making, and facilitate the application of authority. IC reforms guided by bureaucratic theory would involve the creation of formal structures to do this. Environmental theory provides another take on organisational change that can complement bureaucratic theory. It sees exogenous environmental factors as being the key drivers of organisational change.¹²⁵ Environmental theory encompasses the contingency and resource dependency theories. Contingency theory assumes that organisations operate in an open system, where environmental factors strongly influence the way they are structured and led, and how they perform. Environmental factors include the operating environment (eg, threat and legal landscape) and state of technology. Contingency theory also stresses that there is no one model of organisational leadership. Resource dependency theory sees the organisation as operating in a shared environment with other players, with which the organisation interacts while competing for influence and resources.¹²⁶ In the IC context, resource dependency theory would describe the myriad of intelligence agencies in the IC interacting with one another, and jostling for influence and resources.

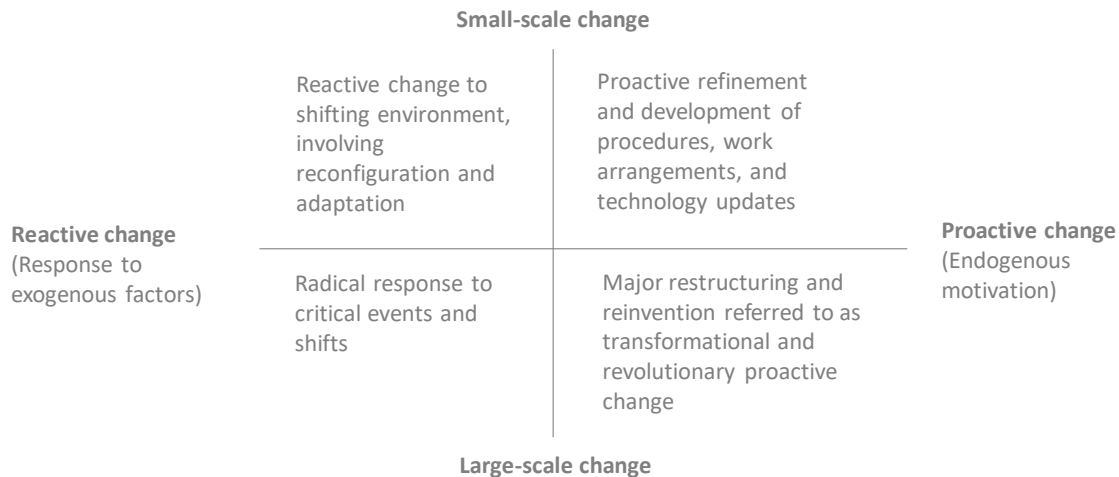
Gill has adapted these concepts to propose a streamlined framework to describe the determinants of intelligence architecture. (Fig. 7.) Gill identifies three determinants influencing intelligence architecture, namely the regime the IC reports to, the IC’s own reform strategy, and technology (which Gill sees as the leading environmental factor). Gill additionally observes that besides the three determinants impacting architecture, IC behaviour can provide feedback on and affect regime behaviour. This might occur if the IC serves as a check-and-balance on the regime, possibly by flagging to policymakers when they overstep their authority. The three determinants also influence one another. For instance, technology influences both regime behaviour and IC strategy, while the regime can influence IC strategy.¹²⁷

Fig. 7: Gill’s framework on intelligence architecture



The Capstone change matrix is useful for classifying intelligence architecture changes, and is used to facilitate the analysis.¹²⁸ The matrix identifies four types of changes, delineated by their magnitude, and whether the changes are proactively initiated or a reaction to environmental changes. (Fig. 8.) This matrix highlights that in parallel to environmental triggers, intelligence reforms can also be proactively initiated due to endogenous motivations, like strategy or performance reviews.

Fig. 8: Capstone change model



Hypothesis

The hypothesis is that changes to intelligence CT architectures since 9/11 have been a reaction to environmental stimuli, like the lingering terrorist threat and government pressure. It is also hypothesised that the architecture changes have been aimed at streamlining and tightening reporting lines within ICs, effectively making ICs more bureaucratic. Such changes would be consistent with bureaucratic and environmental theory.

Findings

Among the countries analysed, the most sweeping changes to intelligence CT architecture were in the US. The first major initiative post-9/11 came quickly in the creation in 2002 of the Department of Homeland Security (DHS) to oversee all aspects of domestic security. Even more fundamental changes followed in 2004, when the Intelligence Reform and Terrorism Prevention Act (IRTPA) created the DNI position at the IC's apex, supported by the Office of the Director of National Intelligence (ODNI).¹²⁹ The DNI post, which was recommended by the 9/11 Commission Report, placed the US' 17-strong IC under the DNI's authority.¹³⁰ The creation of the DNI role meant the termination of the DCI post, and creation of the new DCIA role. This was to split DCI's three main roles (viz, CIA director, US IC head and presidential intelligence adviser) between DCIA and DNI, with the latter two going to DNI.¹³¹ The IRTPA also created the National Counter-terrorism Centre (NCTC) as the US' CT hub in charge of advising the DNI on CT, and overseeing national CT strategy and reporting.¹³²

The UK also implemented changes post-9/11, but they were less extensive than the US's. In 2002, Omand was appointed as Intelligence and Security Coordinator (which later evolved into the role of Permanent Secretary Intelligence, Security, and

Resilience) to bolster top-level bandwidth for managing homeland security.¹³³ 2003 saw the creation of JTAC to handle CT analysis and the issuing of TAs, while bringing together CT expertise from across government. Two further changes emerged following the Butler report. The post of Professional Head of Intelligence Analysis was created in JIC in 2005, to advise the government on intelligence gaps, as well as improve analytical methodology and analysis training. The PM-chaired NSC was created in 2010 to coordinate whole-of-government decision-making on security. Evans said that a motivation for creating NSC was the realisation that the government's decision-making on security had been rather informal, following which NSC was formed to provide a more structured process for channelling intelligence input to policymakers.¹³⁴ Late civil service chief Jeremy Heywood credited the NSC with improving cross-departmental cooperation and efficiency.¹³⁵

Germany's post-9/11 architecture changes have focused on improving coordination, while expanding the role of its military intelligence arm to include more CT coverage. In 2016, Germany appointed a permanent secretary-level Permanent Intelligence Oversight Commissioner (PIOC) to coordinate intelligence priorities and strategy. From 2004-12, Germany set up three multi-agency "fusion centres" to boost cross-agency CT coordination, namely the:

- i. Joint CT Centre (GTAZ) to coordinate efforts against Islamist terrorism, in 2004.
- ii. Joint Internet Centre (GIZ) to detect and dismantle extremist Islamist websites, in 2007.
- iii. Joint CT and Counter-extremism Centre (GETZ) to coordinate efforts on non-Islamist terrorism, counter-intelligence and counter-proliferation, in 2012.

Separately in 2006, Germany set up AntiTerrorDatei, a database of terrorist entities accessible by over three dozen federal and state agencies, to facilitate CT information-sharing. In 2017, the intelligence wing within the military (MAD, or Militärischer Abschirmdienst) was elevated to federal status and placed directly under the defence ministry; MAD's name was also changed to BAMAD (Bundesamt für den Militärischen Abschirmdienst). This elevation enabled BAMAD to take on more responsibilities, including a wider CT coverage, than its MAD precursor. MAD had been mostly focused on counterespionage and operational security for the military. More changes are in the pipeline for Germany following the 2016 Berlin Christmas market attack. The attack was a game-changer for the IC, as it was the deadliest violent incident in Germany since the 1980s. The immediate response was to grow the IC's ranks, and more substantial IC changes are likely to follow.¹³⁶

No recent significant changes have been made to France's intelligence architecture. Post-mortems of the 2015 Paris attacks concluded that intelligence coordination could be improved, and recommended for France to consider creating a lead CT body like the US's NCTC.¹³⁷ But these findings have not led to actual changes.

Reforms through the lens of organisational theory

With regard to bureaucratic theory, the US intelligence architecture has demonstrated an increase in bureaucracy, aimed at streamlining reporting lines and increasing accountability, while rationalising workloads. According to Hastedt and Skelley, the creation of the DNI role reporting to the president was aimed at centralising management of the IC and creating "clear lines of accountability" directly leading to the president. The US reforms considerably increased the size of the intelligence

bureaucracy through the creation of entirely new agencies (eg, DHS, ODNI, NCTC) to handle the heightened CT and coordination demands. On ODNI, Hastedt and Skelley argued that its “elaborate internal structure” is a reflection of the complex US IC ecosystem. They added that high-key bureaucratic reorganisations like the post-9/11 changes in the US have a symbolic element, in assuring the public that the government is acting decisively to prevent a repeat of the events that sparked the reforms.¹³⁸ Even now, terrorism remains a major source of public anxiety¹³⁹, and may continue to fuel further intelligence architecture changes.

In the UK and Germany, the post-9/11 changes have not led to similarly drastic changes in intelligence bureaucracy. Changes have been comparatively smaller in magnitude than the US’s. Neither country has created major new agencies, and both have focused on creating new appointments and multi-agency platforms to boost coordination (eg, UK’s NSC and Germany’s fusion centres), capacity (eg, Germany’s hiring of more IC staff and elevation of BAMAD to federal status) and specific capability. In fact, Germany’s fusion centre concept diverges from the idea of increasing bureaucracy to manage CT. Rather, the concept focuses on making it easier for relevant agencies to bring their existing strengths to the table and form synergistic CT collaborations. GTAZ’s mission statement clarifies that it is a coordination platform with no appointed leader or lead agency, and its formation did not involve the creation of new agencies and laws, or even readjustment of roles and reporting lines.¹⁴⁰

The architecture changes also reflect environmental theory. Seismic shifts in the Western intelligence environment were initiated not only by 9/11, but also the post-Iraq fallout. The key changes in the US (eg, creation of DHS and ODNI and the role of DNI) emerged from these events. Clegg et al noted that the quick creation of DHS post-9/11 is what environmental theory terms an “ad hoc-racy”, where an organisational change arises ad-hoc from external triggers.¹⁴¹ In the UK, the intelligence architecture changes arose from 9/11, the Butler inquiry, and the heightened threat environment in the 2000s. Likewise in Germany, the setting up of CT fusion centres and appointment of the PIOC was a response to the post-9/11 threat environment.

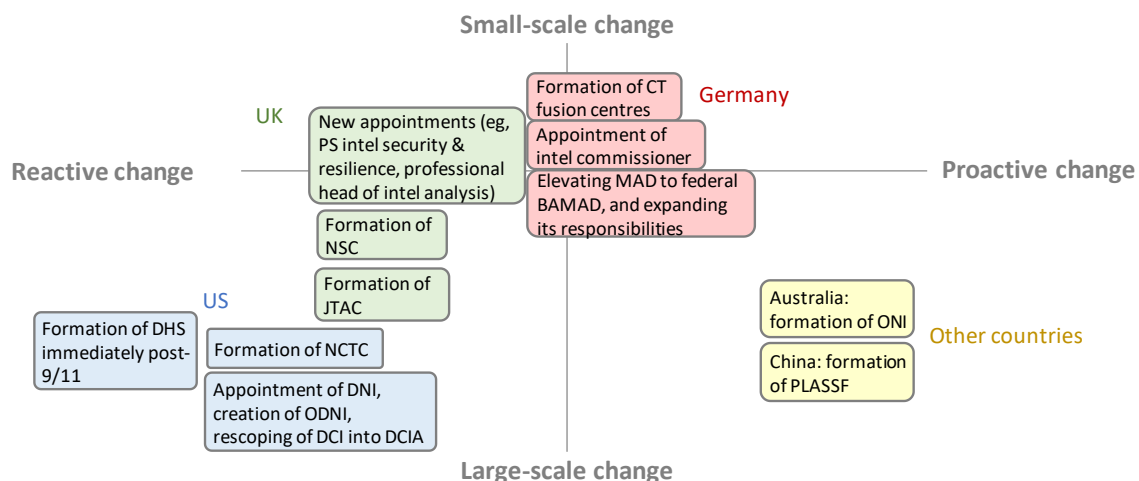
The environmental influences of regime and technology identified by Gill are evident in intelligence architecture reforms. On the regime element, Ryan Shaffer and Jordan Tama have noted that in the US, government commissions can be a vital factor in driving reform, evidenced by the major changes brought about by the 9/11 Commission report. Commissions set up following emergencies enjoy particular influence by virtue of the circumstances surrounding their creation, which they use to push through their change agendas.¹⁴² In France, regime apathy towards the IC has helped keep the status quo, with political leaders displaying no intent to change the intelligence architecture despite some room for improvement. While technology has already heavily influenced IC investment, it is increasingly shaping architecture. A case in point is Germany’s setting up of GIZ.

In line with resource dependency theory, resource constraints affect capacity for reform. The US’ ability to swell its IC ranks and create new agencies has in large part been due to its generous budget. Its 2005 civilian intelligence budget was USD39.8b¹⁴³; in comparison the UK’s 2005 budget was US\$2.5b¹⁴⁴. Even if there is

the will for intelligence reform and structural changes are made, implementation may be hindered by a lack of human resources. Intelligence officers' skillsets, particularly for field agents who take years to develop region-specific expertise and networks, are not fungible and transplantable across theatres. For instance, while the US IC quickly created DHS, it took longer to build a cadre of fluent Arabic speakers.¹⁴⁵ Less visibly, the US IC's rapid post-9/11 growth meant a large proportion of its analysts were initially inexperienced, forcing a trade-off between investing immense effort to train them or reducing the investment in mentoring each analyst. In 2004, 40% of CIA analysts had less than seven years in service.¹⁴⁶

The Capstone matrix is useful for situating intelligence architecture changes. As a group, the changes in the US post-9/11 belong in the quadrant of large-scale changes in reaction to environmental stimuli. The UK's reforms have been smaller in magnitude, but still largely in response to external triggers. Germany's architecture tweaks such as the setting up of the fusion centres and PIOC appointment are minor in magnitude vis-à-vis the US. They also seem more proactive and preventive than the UK's and US's, being made before major terrorist attacks occurred in Germany. To complete the matrix, I found examples from other countries whose intelligence/CT architecture reforms have been both major and proactive. One candidate is Australia's setting up of its Office of National Intelligence (ONI) in 2018 reporting to the PM. ONI is responsible for all-source assessment, OSINT, and overall management of the IC.¹⁴⁷ Another example is China's intelligence reforms from 2015-16, which created the new People's Liberation Army Strategic Support Force (PLASSF) by disbanding another agency and consolidating various collection capabilities. PLASSF was created to place more intelligence resources at the disposal and under more direct control of the PLA.¹⁴⁸ (Fig. 9.)

Fig. 9: Examples of IC changes viewed through Capstone change matrix



Concluding remarks

In the UK, the current intelligence setup will remain in place. Evans noted in April 2019 that there was no drive to radically change the UK's CT approach, as CONTEST remained adaptable and effective.¹⁴⁹ Anderson's report on the 2017 UK attacks did not find the existing CT architecture to be broken.¹⁵⁰ But the US and Germany may consider further refinements of their CT setups. William Nolte and Rosenbach have assessed that while reforms in the US have boosted CT integration and streamlined

processes, there is room for improvement. They argue that further changes may be aimed at enabling the DNI to more effectively assert leadership over the US IC as the DNI is currently hampered by individual agencies retaining significant control over their activities, or helping NCTC perform better in its role of coordinating and leading the US' overall CT effort.¹⁵¹

The findings support the portion of the hypothesis that intelligence CT architecture changes in the countries analysed have been in response to external stimuli like terrorist incidents and government pressure. Deviating from the hypothesis however, the findings show that not all architecture reforms increased the level of bureaucracy. The findings also highlight the relevance of resource dependency theory in explaining how CT architectures are set up.

Discussion

The discussion raises observations arising from the findings. It links the findings on intelligence architecture to the current threat environment, offers takeaways on the intelligence-policy relationship, and identifies intelligence challenges highlighted by the findings.

Challenging threat landscape

ICs have to constantly review their CT roles and how intelligence is configured for CT because of the dynamic threat environment. Approaches that work now may not be sustainable as the threat evolves. ICs may need to revisit stances they regard as “sacred cows”, like the mandate to take lethal action, or involvement in policymaking. Further reconfigurations to intelligence architectures are likely as ICs grapple with emergent threats like the XRW threat.

Three of the key drivers fuelling the threat in the West are the:

- i. Follow-on ISIS threat. Even though ISIS has lost territory, it remains a danger. Evans assesses ISIS to remain a major threat to the UK.¹⁵² A key component of the ISIS threat now comes from “returnees”, or militants returning home or travelling elsewhere. Some gained combat experience and expertise with ISIS. Returnees have launched attacks, like the 2014 attack on the Brussels Jewish museum that killed four. Even if authorities want to prosecute returnees, there may be insufficient evidence to hold up in court.¹⁵³ Europe’s relatively open borders allow returnees to travel easily across the region.¹⁵⁴
- ii. Low-signature attacks by “self-starters”. ISIS’s rise has rallied “self-starters”, or ISIS-inspired individuals or cells to initiate their own attacks. They include the 2016 Nice truck attack.¹⁵⁵ Such attacks are hard to interdict. Attacks launched by clean-skins using everyday items like knives and vehicles as weapons present few opportunities for detection. In comparison, earlier high-signature plots by groups like AQ (eg, the 2006 transatlantic aviation plot) could be detected at various stages, as when operatives travelled or communicated across borders.

- iii. XRW threat. The XRW threat is escalating. While this threat is currently not as severe as jihadist militancy, XRW attacks are becoming increasingly lethal and ambitious. This was illustrated by the 2016 assassination of UK MP Jo Cox, and the lone-shooter attacks in Christchurch and El Paso in 2019 that killed 71. XRW and jihadist movements aggravate each other in a vicious cycle. XRW actions may provoke jihadists to retaliate violently,¹⁵⁶ stimulating further Islamophobia and XRW support. After the 2015 Paris attacks, hate crimes targeting London Muslims tripled.¹⁵⁷

Environmental pressures

Environmental factors will continue to feature in ICs' deliberations. Technology in particular is shaping the intelligence landscape. While technological proliferation has given terrorists more online space to operate, it has also given ICs more tools. Evans notes that the potential for using IT for surveillance, collation and analysis is "enormous", and that the UK's intelligence investment in the last 20 years has mostly been on IT, where a spectrum of CT tools has been developed.¹⁵⁸

The influence of technology has led to architecture changes in some ICs, like Germany's creation of GIZ. The UK's reaction has been more focused on tightening regulation, but structural changes are probably coming. The CT and Border Security Act 2019 (CTBSA) tightened laws on accessing terrorist material, allowing UK-based individuals to be prosecuted for accessing terrorist material just once. The Online Harms White Paper was issued in April 2019 to chart strategies for online regulation. It may eventually lead to intelligence architecture changes to better equip the UK to address online threats while harnessing technology.

Another influence on ICs is the legal environment, which affects how strongly ICs push for more legal powers. Public opposition and controversy over proposed CT laws may scupper them. One area where Western democracies are constrained is in their ability to preventively detain extremists. In Europe, public pressure against preventive detention contributed to the UK abolishing its Imprisonment for Public Protection (IPP) facility allowing for indeterminate detention in 2012. Germany's Constitutional Court likewise ruled preventive detention as unconstitutional in 2011.¹⁵⁹ It is only via a loophole that the US is able to preventatively detain extremists at Guantanamo. It justifies this by claiming that because Guantanamo is in Cuba, detainees do not enjoy similar rights to prisoners on US territory. Emphasising the continuing utility of the facility, Trump signed an executive order to keep it open in 2018, after Obama failed to fulfil his promise to close it. Within the UK, several other areas of CT law are controversial. One area is UK authorities' use of immigration and nationality law to deprive UK nationals of citizenship and passport facilities, like the case of ISIS bride Shamima Begum. Another source of controversy are the UK's new powers under the CTBSA to ban nationals from travelling to terrorist hotspots, which sees the UK taking the unprecedented step of restricting British nationals' movements.

Resource dependency theory will remain relevant in debates on intelligence architecture, as balancing resource limitations is a constant feature of CT. Tradeoffs are needed especially in surveillance. While the UK has over 3,000 persons of terrorism-related interest, it is impossible to constantly monitor them all. There is thus the unavoidable risk that such persons may strike just when they are not being

watched, even if they are known to authorities. Likewise, the US cannot constantly monitor the 1.8 million individuals on its Terrorism Watch List. Resources are further strained by the XRW threat. The UK has elevated XRW threats to the same priority as jihadist threats, which has meant the tough call to divert resources from covering jihadists to monitoring XRW elements. Constraints also apply to Internet regulation. While Germany implemented its hate speech law (Netzwerkdurchsetzungsgesetz) in 2017 to police the Internet, monitoring falls to the police which cannot comprehensively survey the Internet.

Architecture: no standard template

Each CT intelligence configuration has its strengths and drawbacks. ICs consciously or otherwise weigh these when designing their architecture. The drawbacks of having a crowded IC like the US are infighting and turf tussles as agencies jostle for influence, alongside the cost of sustaining this bureaucracy. Inefficiency and redundancy are bugbears. NCTC's CT mission partly overlaps with CIA's.¹⁶⁰ Another overlap is managing liaison relationships, which various agencies including ODNI and CIA are involved in.¹⁶¹ On analysis, aggressive inter-agency competition raises the risk of politicisation, as agencies may prioritise winning the leadership's confidence over maintaining analytical integrity.¹⁶² Arguing over shared assessments also leads to time-consuming "analysis paralysis"¹⁶³, and the watering down of assessments resulting in less incisive products.¹⁶⁴ But inter-agency competition has benefits. Jackson thinks the adversarial culture in the US IC allows room for more independent viewpoints to be explored, which boosts analytical rigour.¹⁶⁵

In comparison, the UK's IC is more streamlined and appears less adversarial. It therefore suffers from less infighting and requires fewer resources to sustain.¹⁶⁶ Because there are fewer agencies in the UK, UK agencies occupy larger footprints in their IC, relative to their US counterparts' positions in the US IC. For instance, GCHQ's influence in the UK IC would be relatively larger than NSA's in the US. With less competition for status, UK agencies may be less incentivised to engage in politicking to gain influence.¹⁶⁷ But the risk of centralising analysis in a single JIC, alongside the more "collegial" atmosphere in the UK IC, is groupthink.¹⁶⁸ This can lead to threats being missed if alternate hypotheses are overlooked, or the Joint Intelligence Office (JIO) as a group dismisses important evidence. Jackson adds that a related drawback from the UK IC's "laser focus" on consumer priorities is a generally less conducive environment for encouraging independent analysis or horizon scanning, despite these exercises being useful for spotting new threat dimensions.¹⁶⁹

Takeaways on the intelligence-policy relationship

While tensions in the intelligence-policy relationship are inevitable, protracted rifts are damaging as they hamper intelligence work. Deep rifts might manifest in policymakers ignoring intelligence advice or stymying CT actions, an IC distracted by the need to constantly engage a sceptical policymaker audience, and stark differences in views on key issues between the IC and its political masters that may get aired in public. Such indications have continued to surface in the US after Iraq. In mid-2019, the Trump administration alleged active collaboration between Iran and AQ, which the IC doubts is the case.¹⁷⁰ The US IC earlier voiced wariness of Obama, who publicly blamed it for failing to predict ISIS's emergence and Muammar Gaddafi's fall in Libya

sooner¹⁷¹, and was seen as not being quick to defend NSA's surveillance activities following the Snowden leaks.¹⁷²

Going forward, ICs and policymakers need to iron out approaches to several key issues. One issue is how widely CT intelligence should be shared. For instance, CT efforts would be helped if police are told of locations under their beat that are of intelligence interest, like gyms where extremists congregate. The danger of widening access to privileged information is that sensitive sources may be compromised. In governments where inter-agency competition is bitter, information-sharing may be hindered by agencies tussling for recognition through information scoops.¹⁷³ Configuring architecture to force information-sharing may alleviate this, like Germany's setting up of CT fusion centres.¹⁷⁴ Harder still for governments is weighing the risk of sharing intelligence with foreign agencies and industry collaborators, even though such collaborations often yield quick returns.¹⁷⁵ While information-sharing between the US and EU or within the Five Eyes¹⁷⁶ is extensive, ICs will be reluctant to share intelligence with hostile neighbours that may endanger their sources there. Separately, industry collaborations run the risk of contractors leaking information.

The intelligence-policy debate raises the question of how IC chiefs are selected. Chiefs have a key role in holding the line against policymakers trying to pressure the IC into situations that compromise their integrity, like policy advocacy. For this reason, the House of Commons' response to the Chilcot report recommended that JIC chairmen be appointed only after reaching the apex of their careers at permanent secretary-level, when they are no longer eligible for promotion.¹⁷⁷ This ensures they have little to gain by succumbing to policymakers' pressure. While this is feasible in the UK, it may not be tenable in countries like the US where IC leadership appointments are now highly political.¹⁷⁸

The findings underscore the need for sound analytical practices to mitigate the risk of analytical politicisation. The Iraq episode prompted a push to raise analytical standards in the US and UK ICs. ODNI tightened analytical fundamentals including source vetting, considering alternatives and emphasising accuracy.¹⁷⁹ The Chilcot report stressed the need for UK agencies to uphold tenets like ensuring precision in the reporting of facts, assessments and probabilities.¹⁸⁰ Other measures include the use of designated "devil's advocates", by agencies like Israel's MOSSAD, to systematise the examination of alternative perspectives.¹⁸¹ Agencies like CIA rely on ombudsmen to surface analytical impropriety and politicised reporting.¹⁸² Researchers have increasingly noted that methodology must be complemented by a healthy analysis culture. Stephen Marrin suggests that to prevent corruption, intelligence needs to develop a "strong sense of professional identity and integrity".¹⁸³ But malpractice sometimes continues to be rewarded. The US analysts who supplied politicised reporting on Iraq were not censured, and were routinely rewarded for service.¹⁸⁴ There is an additional consumer management element to ensuring analytical integrity. A perennial question is whether ICs should allow policymakers access to raw reports. Doing so may encourage policymakers to form opinions on or predispose them to favouring some sources (eg, HUMINT over TECHINT). This may interfere with intelligence reporting if the IC starts to rely more on the policymakers' favoured sources for reporting, which was evident in the US IC's reporting in the run-up to the Iraq invasion.

Longer-term intelligence challenges

Beyond tactical threats, counter-ideology is potentially the toughest CT issue to tackle, on which the IC's role is debated. Evans views the Prevent strand that encompasses counter-ideology as the hardest element of CONTEST.¹⁸⁵ Many governments are still playing catch-up. A retired senior security official said that as of April 2019, the UK still lacked the "toolbox" and "networks"¹⁸⁶ for counter-ideology, partly arising from its earlier reluctance to involve itself in religious issues. It has only been more recently that the UK government has started to view counter-ideology as its responsibility. For now, the UK and Germany have not involved intelligence in fronting counter-ideology. MI5 decided against participating in community engagement as it might distract from MI5's core work.¹⁸⁷ The XRW phenomenon poses a growing counter-ideology challenge and requires its own counter-narratives.¹⁸⁸ One obstacle in democracies is dealing with individuals who express extremist views but stop short of inciting violence. The senior security official said that UK-based extremists take advantage of the "raucous public sphere", as "freedom of speech comes first".¹⁸⁹

Various countries have made progress on CT coordination both internally and with foreign partners, but collaborations will continue to be complicated by differences in systems and values. Evans observed that coordination between the UK's intelligence agencies "greatly improved" in the last decade, fostering a "greater sense of an IC" with MI5 and MI6 acting more as "one coordinated entity". Previously, UK agencies tended to act as "tribal groups" with professional but limited engagement, among whom coordination was hampered by non-uniform practices.¹⁹⁰ Omand noted that CT policymaking is complicated as it demands working across numerous stakeholders.¹⁹¹ International collaboration is tougher. Evans recalled that UK CT collaboration with European partners is occasionally complicated by differences in law, and collaboration with countries with drastically different approaches to CT and rights is trickier.¹⁹²

Complications in the intelligence-policy relationship might arise if policymakers stretch the definition of terrorism. Policymakers may label political opponents or protestors as terrorists, even if they do not fit the conventional definitions of terrorism. This would compel the IC to use CT powers to act against such entities, although the IC may have reservations about categorising them as terrorists. The ongoing 2019 Hongkong protests illustrate how this might happen. After months of protests, Chinese authorities have started to insinuate that the protestors are terrorists. This has been complemented by a concerted CT-style counter-ideology campaign against the protests. In August 2019, state TV played slick counternarrative videos showing CT assets being prepared and calling for "evil" to be eliminated.¹⁹³ China's IC would not oppose the use of its CT mandate in this instance. But in a democratic context where the IC is not entirely pliable, the IC might oppose the use of its CT powers against political opponents when it is unclear if they can be defined as terrorists.

Conclusion

The terrorism threat is becoming more multi-dimensional and complex. The acute jihadist threat has evolved from being focused around core groups like AQ and ISIS to being diffused across disparate players. Meanwhile, the XRW threat has become increasingly severe. I hypothesised that these realities would compel ICs to adopt

additional CT roles beyond the intelligence cycle that leverage on their strengths. The findings corroborated this. Some agencies are authorised to take lethal actions against terrorists. Governments use intelligence agencies to negotiate terrorist hostage releases, and for informal diplomacy like discreet CT collaborations. Another growth area is intelligence-industry collaboration to build CT capability. But ICs remain reluctant to engage in counter-ideology, to avoid getting embroiled in controversy and criticism. But despite these additional responsibilities, ICs' primary preoccupations will remain the mainstays of collecting and reporting intelligence.

On the intelligence-policy relationship, I hypothesised that ICs in democracies would seek to maintain some distance from policymaking with the controversy over Iraq still fresh. The findings supported this. In the UK and Germany, there is strict intelligence-policy separation, maintained by professionalism, role definition, alongside pre-existing work culture and norms. Different drivers feature in the US and France, where distrust between politicians and ICs presently prevents both sides from drawing close. Since Iraq, ICs in countries like the US and UK have tried to mitigate the risk of intelligence politicisation. The increasingly frequent election of unfamiliar political players will complicate the intelligence-policy relationship. ICs would need to educate fresh faces on the nature of intelligence and their role as consumers, before they can in turn provide effective direction. Fortunately, the appointment of Boris Johnson as UK PM may mean status quo for the UK IC, which Johnson is familiar with having overseen MI6 as foreign secretary.

There is no standard CT intelligence architecture template. Each configuration has its benefits and tradeoffs. The US made wide-ranging changes to its architecture post-9/11, growing its size and level of bureaucracy. Its gargantuan machinery possesses huge capability and reach, promotes a vibrant analytical culture, but means more costs and infighting. The UK's more streamlined configuration and comparatively minor tweaks to its architecture post-9/11 have similarly proven effective. The UK's unique JIC confers the advantage of ensuring policymakers are constantly updated on intelligence perspectives. But the JIC approach only works with a professional and competent civil service whose bureaucrats can compartmentalise their JIC and policymaker responsibilities, and fulfil both competently. In Germany, recent CT architecture changes have been focused on growing multi-agency coordination, namely through the creation of CT fusion centres. There are no plans to amend France's CT architecture.

This paper flagged areas for further research. Intelligence theory is lacking in areas outside the intelligence cycle, like the intelligence-policy relationship and IC management. The intelligence-policy relationship needs further examination vis-a-vis developments on both sides of the divide. They include the growing complexity of intelligence work, the emergence of new collection fields with contentious policy angles like SOCMINT, and increasingly unpredictable political landscapes. CT architecture merits more research to examine the value propositions of the different CT configurations in key countries, for which analytical frameworks can be drawn from organisational theory.

---oOo---

(Dedicated to Dr Mark Currie, who supervised the initial research and helped secure the interviews with Sir David Omand and Lord Jonathan Evans, but passed before this paper was completed.)

-
- 1 Lomas and Murphy, "Intelligence and Espionage," 42.
 - 2 Omand and Phythian, "Ethics and Intelligence," 49.
 - 3 Sims, "Decision Advantage," 389-403.
 - 4 Lowenthal, *Secrets to Policy*, 283.
 - 5 Lomas and Murphy, 42.
 - 6 Ibid.
 - 7 Lowenthal, 281.
 - 8 Davis, "Sherman Kent's Final Thoughts," 3.
 - 9 Rovner, "Is Politicisation Ever a Good Thing," 56.
 - 10 Gill, "Theories of Intelligence," 43.
 - 11 Betts, "Analysis," 87-100; Warner, "Risk Shifting," 16-19.
 - 12 Marrin, "Evaluating Intelligence Theories," 481.
 - 13 Johnson, "Sketches for a Theory," 33-53.
 - 14 Treverton, "Theory and Practice," 473-4.
 - 15 Phythian, "Intelligence Theory," 68.
 - 16 Hastedt, "NSA Intelligence Gathering," 1-6.
 - 17 Kettl, *Administrative Process*, 268.
 - 18 Davis, "Kent-Kendall Debate," 91; Hulnick, "Relations Between Intelligence Producers and Policy," 130.
 - 19 Heymann, "Intelligence/Policy Relationships," 57.
 - 20 Lowenthal, 258; Marrin, "Revisiting Intelligence," 1-24.
 - 21 Davis, 91-96.
 - 22 Lowenthal, 281-85.
 - 23 Jervis, "Why Intelligence and Policymakers Clash," 190.
 - 24 Lowenthal, 282.
 - 25 Lowenthal, "Policymaker-Intelligence Relationship," 444.
 - 26 Lowenthal, *Secrets to Policy*, 299.
 - 27 Lomas and Murphy, 42-56.
 - 28 Rovner, 62-63.
 - 29 Hulnick, 132.
 - 30 Jervis, 203.
 - 31 Davis, 93.
 - 32 Rosenbach, "Incisive Fight," 138.
 - 33 Betts, "American Strategic Intelligence," 258-59.
 - 34 Davis, 93.
 - 35 Butler report, 1.
 - 36 Craddock, *Know Your Enemy*, 296.
 - 37 Ben-Haim, "Policy Neutrality and Uncertainty," 980-81.
 - 38 Lomas and Murphy, 42.
 - 39 Marrin, 2.
 - 40 Hulnick, 130-31.
 - 41 Rovner, 57.
 - 42 Marrin, "Analytic Politicisation," 33-34.
 - 43 Lowenthal, 292.
 - 44 Hastedt, "Politics of Intelligence," 12.
 - 45 Gill and Phythian, "Insecure World," 133.
 - 46 Lomas and Murphy, 42.
 - 47 Lowenthal, 286.
 - 48 Marrin, 37.
 - 49 Bar-Joseph and Levy, "Conscious Action," 474.
 - 50 Jervis, 200.
 - 51 Coletta, "Politicising Intelligence," 75-76.
 - 52 Lowenthal, 283.
 - 53 Hastedt, 9.
 - 54 Davis, 2-5.

55 Omand, "SOCMINT," 355-72.
56 Hulnick, 143.
57 Davis, "Kent's Final Thoughts," 2-3.
58 Davis, "Kent-Kendall Debate," 99.
59 Rovner, 57-58.
60 'SWOT' stands for Strengths, Weaknesses, Opportunities and Threats analysis.
61 'TOWS' is a matrix derived from SWOT analysis, to identify four further types of business strategies.
62 McKinsey, "Growing Beyond"; Zook, "New Rules."
63 Evans (Michael), "CIA Wins Back Control."
64 Henry, "Francois Hollande."
65 Coroner's Inquests into the Deaths of Diana and Dodi al-Fayed.
66 *Spiegel*, "German Intelligence."
67 Evans, lecture in St Andrews on April 15, 2019.
68 *Intelligence Online*, "DCRI."
69 Cobain, "UK Hostage Strategy."
70 Sherlock, "Taliban Members Released."
71 Javid, speech on June 4, 2018.
72 Alexander Younger, speech at St Andrews on December 3, 2018.
73 White House, National Strategy for CT 2018.
74 Palantir, "CIA-Funded."
75 Williamson, "How France Hopes to Help."
76 Zenko, "America's Virulent."
77 Lowenthal, 481.
78 Dahl, 88-90.
79 Omand, interview.
80 Omand, "SOCMINT."
81 Gill, 43-44.
82 Pillar, "Intelligence, Policy."
83 Fingar, *Reducing Uncertainty*, 45-6.
84 Lomas and Murphy, 120.
85 Bruce and George, "Intelligence Analysis," 12.
86 Rovner, 65-67.
87 Miller, "Trump's Refusal."
88 Dreazen and Naylor, "Mission Unstoppable."
89 Obama's speech at CIA, April 20, 2009.
90 Legrand, "More Symbolic," 362.
91 Bouchnik-Chen.
92 Omand, interview.
93 Chilcot report, 133.
94 Omand.
95 *Ibid.*
96 Chilcot report, 734-35.
97 Omand.
98 Senior security officer, interview.
99 Omand.
100 Evans, interview.
101 The September Dossier's full name is "Iraq's Weapons of Mass Destruction: The Assessment of the British Government". It was prepared by JIC and issued by the UK government on 24 Sep 02 on the day parliament was recalled to discuss its contents, which claimed evidence that Iraq had resumed its WMD programme.
102 Lomas and Murphy, 53.
103 Chilcot report, 131 and 900.
104 Evans.
105 Chilcot report, 881.
106 Chilcot statement on July 6, 2016.
107 Evans.
108 Morrison, "British Intelligence Failures," 513.
109 Jackson, interview.
110 *Deutsche Welle*, "AfD Wins Case."
111 Rauffer, interview.

-
- 112 Evans.
113 Omand, "Time to Move Beyond the Intelligence Cycle?" 139-40.
114 Arcos and Palacios, "Impact of Intelligence on Decisionmaking," 749.
115 Omand, interview.
116 Raufur.
117 Chilcot report, 279.
118 Lomas and Murphy, 52-53.
119 Pillar.
120 Ibid.
121 Pillar, "Intelligence and US Foreign Policy," 120.
122 Chilcot report, 74 and 860.
123 Anderson, *Attacks in London and Manchester*.
124 Hastedt and Skelley, "Intelligence in a Turbulent World," 115.
125 Ibid., 115-121.
126 Clegg, Kornberger and Pitsis, 520-23.
127 Gill, "Way Ahead," 580.
128 Clegg, Kornberger and Pitsis, 373,
129 Omand, "Creating Intelligence Communities," 107.
130 Tama, *Terrorism and National Security Reform*, 139.
131 Negroponte and Wittenstein, 381-86.
132 Rosenbach, 136.
133 Omand, 108.
134 Evans.
135 House of Commons, *Lessons Still to be Learned*, 15.
136 Steinberg, "German Inefficiency"; Eddy, "A Year After the Berlin Market Attack."
137 Simcox, "French Intelligence Reform."
138 Hastedt and Skelley, 114.
139 Dearlove, "National Security and Public Anxiety," 37.
140 BfV, "GTAZ."
141 Clegg, Kornberger and Pitsis, 527-8.
142 Shaffer, "CT Intelligence," 181.
143 ODNI letter to Steven Aftergood.
144 *Economist*, "Britain's Intelligence Services."
145 Saner, "Former FBI Agent."
146 Gentry, "New Form of Politicisation," 664.
147 ONI, "Overview."
148 Mattis, "China Reorients."
149 Evans.
150 Anderson.
151 Nolte, 615-17; Rosenbach, 136.
152 Evans, lecture.
153 Ibid.
154 Raufur.
155 Byman, "ISIS's Next Move," 29.
156 Evans, interview.
157 Byman, 31.
158 Evans, lecture.
159 *Deutsche Welle*, "Preventive Detention."
160 Rosenbach, 137.
161 Negroponte and Wittenstein, 391.
162 Bar-Joseph, "Politicisation of Intelligence," 361-62.
163 Coletta, 66-67.
164 Betts, 260.
165 Jackson.
166 Ibid.
167 Nolte, "US Intelligence," 617.
168 Coletta, 66-67.
169 Jackson.
170 Hirsh, "US Intelligence Undercuts".
171 Bouchnik-Chen; Lowenthal, *Intelligence*, 285.

-
- 172 Gentry, 654.
173 Dearstyne, "Fighting Terrorism," 178.
174 Lambert, "Addressing Challenge," 3.
175 Davies, 291.
176 The 'Five Eyes' refers to the Anglophone intelligence alliance that includes the US, UK, Canada, Australia and New Zealand.
177 House of Commons, "Lessons," 77.
178 Bar-Joseph and Levy, 474.
179 Lowenthal, "Policymaker-Intelligence Relationship," 444.
180 Chilcot report, 131.
181 Pascovich, "Devil's Advocate," 1-9.
182 Pillar, "Intelligence, Policy."
183 Marrin, 53-54.
184 Hastedt and Skelley, 126.
185 Evans.
186 Senior security official.
187 Evans.
188 Ibid.
189 Senior security official.
190 Evans.
191 Omand.
192 Evans.
193 CCTV, "Say No to Riots!"

Bibliography

1. Anderson, David. *A Question of Trust: Report of the Investigatory Powers Review*. London: Williams Lea Group, June 2015.
2. Anderson, David. *Attacks in London and Manchester: March-June 2017: Independent Assessment of MI5 and Police Internal Reviews*. Home Office, December 5, 2017. <https://www.gov.uk/government/publications/attacks-in-london-and-manchester-between-march-and-june-2017>. Accessed June 28, 2018.
3. Anderson, David. *Citizenship Removal Resulting in Statelessness*. Williams Lea Group: London, April 2016.
4. Anderson, David. "CJEC Judgement in Watson/Tele2." David Anderson QC. <https://www.daqc.co.uk/2017/04/11/cjeu-judgment-in-watson>. Accessed June 28, 2019.
5. Anderson, David. *Deportation with Assurances*. Williams Lea Group: London, July 2017.
6. Anderson, David. "Extremism and the Law." Treasurer's Lecture, Middle Temple Hall, March 18, 2019.
7. Anderson, David. "Human Rights and the Future of Surveillance." David Anderson QC. <https://www.daqc.co.uk/2018/10/26/human-rights-and-the-future-of-surveillance>. Accessed June 28, 2019.
8. Anderson, David. "Intelligence Handling and the Recent Terrorist Attacks." David Anderson QC. www.daqc.co.uk/2017/06/28/recent-terrorist-attacks-police-and-mi5-reviews. Accessed June 28, 2019.
9. Anderson, David. "David Anderson QC: Prevent Strategy Can Work Against Radicalisation... If it is Trusted." *Evening Standard*, June 17, 2019.
10. Anderson, David. *Report of the Bulk Powers Review*. London: Williams Lea Group, August 2016.
11. Anderson, David. "Reporting Terrorism." Exeter University Annual Journalism Lecture, February 11, 2019.
12. Anderson, David. "Shades of Independent Review." David Anderson QC. December 6, 2017. <https://www.daqc.co.uk/2017/12/06/shades-independent-review>. Accessed June 28, 2019.
13. Anderson, David. "Shielding the Compass: How to Fight Terrorism Without Defeating the Law." *European Human Rights Law Review*, June 15, 2013.
14. Anderson, David. "Statement by David Anderson QC on Publication of his report: 'Attacks in London and Manchester – March-June 2017'." December 5,

2017. <https://www.daqc.co.uk/wp-content/uploads/sites/22/2017/12/press-release.pdf>. Accessed June 28, 2019.
15. Anderson, David. "Terrorism: the EU Picture." *Counsel Magazine*, May 2017.
 16. Anderson, David. "Terrorism and National Security." Lecture, February 22, 2017. <https://rusi.org/event/terrorism-and-national-security-0>. Accessed June 28, 2019.
 17. Anderson, David. "Terrorism, Tolerance and Human Rights." Speech in Strasbourg, October 11, 2016.
 18. Anderson, David. "The Fly in the China Shop." British Embassy Lecture on International Law, The Hague, September 26, 2018.
 19. Anderson, David. "The Investigatory Powers Act 2016 – An Exercise in Democracy." David Anderson QC, December 3, 2016. <https://www.daqc.co.uk/2016/12/03/the-investigatory-powers-act-2016-an-exercise-in-democracy>. Accessed June 28, 2019.
 20. Anderson, David. "The Qatada Complex." David Anderson QC, July 20, 2017. <https://www.daqc.co.uk/2017/07/20/the-qatada-complex>. Accessed June 28, 2019.
 21. Anderson, David. *The Terrorism Acts in 2013*. London: Williams Lea Group, July 2014.
 22. Anderson, David. "There are Limits to Tolerance, but Human Rights are Key to Democracy." *Prospect*, June 7, 2017.
 23. Anderson, David. "Who Governs the Internet?" *Counsel Magazine*, May 2018.
 24. Aldrich, Richard J. "US-European Intelligence Cooperation on Counter-Terrorism: Low Politics and Compulsion." *British Journal of Politics and International Relations* 11 (2009): 122-39.
 25. Aly, Anne. "The Policy Response to Home-Grown Terrorism: Reconceptualising *Prevent* and *Resilience* as Collective Resistance." *Journal of Policing, Intelligence and Counter Terrorism* 8, no. 1 (2013): 2-18.
 26. Arcos, Ruben, and Jose-Miguel Palacios. "The Impact of Intelligence on Decision-Making: The EU and the Arab Spring." *Intelligence and National Security* 33, no. 5 (2018): 737-54.
 27. Argomaniz, Javier, Oldrich Bures, and Christian Kaunert. "A Decade of EU Counter-Terrorism and Intelligence: A Critical Assessment." *Intelligence and National Security* 30, no. 2-3 (2015): 191-206.

28. Bar-Joseph, Uri. "The Politicization of Intelligence: A Comparative Study." *International Journal of Intelligence and Counter Intelligence* 26, no. 2 (2013): 347-69.
29. Bar-Joseph, Uri, and Jack S. Levy. "Conscious Action and Intelligence Failure." *Political Science Quarterly* 124, no. 3 (2009): 461-88.
30. Baudino, Claudio, Nicole Roberta Giuggioli, Rossella Briano, Stefano Massaglia, and Christiana Peano. "Integrated Methodologies (SWOT, TOWS, LCA) for Improving Production Chains and Environmental Sustainability of Kiwifruit and Baby Kiwi in Italy." *Sustainability* 9, no. 1621 (2017).
31. *BBC*. "Brown Defends Hostages Strategy." June 22, 2009. <http://news.bbc.co.uk/1/hi/uk/8112057.stm>. Accessed July 11, 2019.
32. Beaumont, Peter. "French Secret Service Hostage and Soldiers Killed in Somali Rescue Mission." *Guardian*, January 12, 2013.
33. Bejesky, Robert. "The SSCI Investigation of the Iraq War: Part II: Politicisation of Intelligence." *Southern University Law Review* 40, no. 2 (2013): 243-92.
34. Ben-Haim Yakov. "Policy Neutrality and Uncertainty: An Info-Gap Perspective." *Intelligence and National Security* 31, no. 7 (2016): 978-92.
35. Bellovin, Steven M. "By Any Means Possible: How Intelligence Agencies Have Gotten Their Data." *Intelligent Systems* (July/August 2014): 80-84.
36. Betts, Richard K. "Analysis, War and Decision: Why Intelligence Failures are Inevitable." In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 87-111. Abingdon: Routledge, 2009.
37. Betts, Richard K. "American Strategic Intelligence: Politics, Priorities and Direction." In *Intelligence Policy and National Security*, edited by Robert L. Pfaltzgraff Jr., Uri Ra'anan, and Warren Milberg, 245-67. Hong Kong: Macmillan, 1981.
38. Boer, Monica Den. "Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis." *Intelligence and National Security* 30, no. 2-3 (2015): 402-19.
39. Borer, Douglas A. "Problems in the Intelligence-Policy Nexus: Rethinking Korea, Tet, and Afghanistan." *Intelligence and National Security* 29, no. 6 (2014): 811-36.
40. Bouchnik-Chen, Raphael G. "Avoiding the Politicisation of Intelligence and Policy-Making." *Begin-Sadat Centre for Strategic Studies*, March 4, 2019. <https://besacenter.org/perspectives-papers/intelligence-politicization>.

41. Bruce, James B., and Roger Z. George. "Intelligence Analysis: What is it – And What Does it Take?" in *Analyzing Intelligence: National Security Practitioners' Perspectives*, edited by Roger Z. George and James B. Bruce, 1-22. Washington DC: Georgetown University Press, 2014.
42. Bruce, James B., and Roger Z. George. "Professionalising Intelligence Analysis." *Journal of Strategic Security* 8, no. 3 (2015): 1-23.
43. Bundesamt für Verfassungsschutz. "Gemeinsames Terrorismusabwehrzentrum (GTAZ – Joint Counter-Terrorism Centre)." <https://www.verfassungsschutz.de/en/fields-of-work/islamism-and-islamist-terrorism/gtaz-en>. Accessed July 14, 2019.
44. Byman, Daniel. "ISIS's Next Move." *National Interest* (January/February 2018): 25-33.
45. Cabinet Office. *Review of Intelligence on Weapons of Mass Destruction: Implementation of its Conclusions*. March 2005. CM6492.
46. Castle, Stephen. "Analysis: Britain's Iraq War Inquiry." *New York Times*, July 6, 2016.
47. Caudillo, Francisco, Skief Houben, and JehanZeb Noor. "Growing Beyond the Core Business." McKinsey. July 2015. <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/growing-beyond-the-core-business>. Accessed July 11, 2019.
48. CCTV English. "Say No to Riots! Say No to Evil! Say No to Hong Kong Independence!" August 11, 2019. <https://www.youtube.com/watch?v=LyEANMz7nls>.
49. Chilcot, John. "Statement by Sir John Chilcot: 6 July 2016." The Iraq Inquiry. https://webarchive.nationalarchives.gov.uk/20171123122743tf_/http://www.iraqinquiry.org.uk/the-report. Accessed June 6, 2019.
50. Cimbala, Stephen J. "Introduction." In *Intelligence and Intelligence Policy in a Democratic Society*, edited by Stephen J. Cimbala, 1-24. US: Transnational Publishers, 1987.
51. Clegg, Stewart, Martin Kornberger, and Tyrone Pitsis. *Managing and Organisations*. London: Sage Publications, 2011.
52. Cobain, Ian. "UK Hostage Strategy Scrutinised After ISIS Threatens Fifth Western Hostage." *Guardian*, October 8, 2014.
53. Coletta, Giovanni. "Politicising Intelligence: What Went Wrong With the UK and US Assessments on Iraqi WMD in 2002." *Journal of Intelligence History* 17, no. 1 (2018): 65-78.

54. Committee of Privy Counsellors. *Review of Intelligence on Weapons of Mass Destruction (Butler Report)*. July 14, 2004. HC898.
55. Committee of Privy Councillors. *The Report of the Iraq Inquiry (Chilcot Report)*. July 6, 2016. HC264.
56. Dahl, Erik J. "Why Won't They Listen? Comparing Receptivity Toward Intelligence at Pearl Harbor and Midway." *Intelligence and National Security* 28, no. 1 (2013): 68-90.
57. Davies, Philip H. J. "Theory and Intelligence Reconsidered." In *Intelligence Theory—Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 186-207. Abingdon: Routledge, 2009.
58. Davies, Philip H. J. *MI6 and the Machinery of Spying*. London: Frank Cass, 2004.
59. Davies, William Adair. "Counterterrorism Effectiveness to Jihadists in Western Europe and the United States: We Are Losing the War on Terror." *Studies in Conflict and Terrorism* 41, no. 4 (2018): 281-96.
60. Davis, Jack. "Sherman Kent's Final Thoughts on Analyst-Policymaker Relations." *The Sherman Kent Centre for Intelligence Analysis Occasional Papers* 2, no. 3 (June 2003): 1-11.
61. Davis, Jack. "The Kent-Kendall Debate of 1949." CIA. <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol35no2/pdf/v35i2a06p.pdf>. Accessed June 9, 2019.
62. Dean, Neville. "Butler Report: Key Findings." *Independent*, July 14, 2004.
63. Dearlove, Richard. "National Security and Public Anxiety: Our Changing Perceptions." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 33-42. Oxford: Oxford University Press, 2012.
64. Dearstyne, Bruce W. "Fighting Terrorism, Making War: Critical Insights in the Management of Information and Intelligence." *Government Information Quarterly* 22, no. 2 (December 2005): 170-86.
65. Degaut, Marcos. "Spies and Policymakers: Intelligence in the Information Age." *Intelligence and National Security* 31, no. 4 (2016): 509-31.
66. *Deutsche Welle*. "AfD Wins Case Against Spy Agency." February 26, 2019.
67. *Deutsche Welle*, "German Court Rules Preventive Detention Unconstitutional." May 4, 2011.
68. Devanny, Joe, Robert Dover, Michael S. Goodman, and David Omand. "Why the British Government Must Invest in the Next Generation of Intelligence Analysts." *RUSI Journal* 163, no. 6 (2018): 78-89.

69. Dillon, Robin L., Genevieve Lester, Richard S. John, and Catherine H. Tinsley. "Differentiating Conflicts in Beliefs Versus Value Tradeoffs in the Domestic Intelligence Policy Debate." *Risk Analysis* 32, no. 4 (2012): 713-28.
70. Drezzen, Yochi, and Sean D. Naylor. "Mission Impossible: Why is the CIA Running America's Foreign Policy?" *Foreign Policy*, May 18, 2015.
71. Dylan, Huw. "Secret Interventions and Clandestine Diplomacy." In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael S. Goodman, 335-54. London: Palgrave Macmillan, 2017.
72. *Economist*. "Britain's Intelligence Services: Cat's Eyes in the Dark." March 17, 2005.
73. Eddy, Melissa. "A Year After the Berlin Market Attack, Germany Admits Mistakes." *New York Times*, December 19, 2017.
74. Eiran, Ehud. "The Three Tensions of Investigating Intelligence Failures." *Intelligence and National Security* 31, no. 4 (2016): 598-618.
75. Eisenfeld, Beth. "The Intelligence Dilemma: Proximity and Politicization – Analysis of External Influences." *Journal of Strategic Security* 10, no. 2 (2017): 77-96.
76. Eriksson, Gunilla. "A Theoretical Reframing of the Intelligence-Policy Relation." *Intelligence and National Security* 33, no. 4 (2018): 553-61.
77. Evans, Michael. "CIA Wins Back Control of Drone Strikes." *Times*, March 15, 2017.
78. Evans, Jonathan. "Guest Lecture." Guest Lecture for Module on Fundamentals of Terrorist Violence (IR5924), University of St Andrews, April 15, 2019.
79. Evans, Jonathan. Interview with David Chen. Personal Interview. St Andrews, April 16, 2019.
80. Gardham, Duncan. "Does MI6 Have a Licence to Kill?" *Telegraph*, December 3, 2012.
81. Gentry, John A. "A New Form of Politicization? Has the CIA Become Institutionally Biased or Politicized?" *International Journal of Intelligence and Counterintelligence* 31, no. 4 (2018): 647-80.
82. Gentry, John A. "Assessing Intelligence Performance." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 87-106. Oxford: Oxford University Press, 2012.

83. Gill, Peter. "Theories of Intelligence." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 43-58. Oxford: Oxford University Press, 2012.
84. Gill, Peter. "Theories of Intelligence: Where are We, Where Should We Go and How Might We Proceed?" In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 54-72. Abingdon: Routledge, 2009.
85. Gill, Peter. "The Way Ahead in Explaining Intelligence Organisation and Process." *Intelligence and National Security* 33, no. 4 (2018): 574-86.
86. Gill, Peter, and Mark Phythian. "Developing Intelligence Theory." *Intelligence and National Security* 33, no. 4 (2018): 467-71.
87. Gill, Peter, and Mark Phythian. *Intelligence in an Insecure World*. Cambridge: Polity Press, 2006.
88. Gill, Peter, Stephen Marrin, and Mark Phythian. "Introduction." In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 1-3. Abingdon: Routledge, 2009.
89. Glees, Anthony, Philip H. J. Davies, and John N. L. Morrison. *The Open Side of Secrecy*. London: Social Affairs Unit, 2006.
90. Gleeson, Dennis. "The High Cost of Politicising Intelligence." *The Atlantic*, February 25, 2017.
91. Gookins, Amanda J. "The Role of Intelligence in Policy Making." *SAIS Review of International Affairs* 28, no. 1 (Winter-Spring 2008): 65-73.
92. Hanni, Adrian. "When Casey's Blood Pressure Rose: A Case Study of Intelligence Politicisation in the United States." *Intelligence and National Security* 31, no. 7 (2016): 963-77.
93. Harris, Shane. "'No One's Really in Charge' in Hostage Negotiations." *Foreign Policy*, October 9, 2014.
94. Hastedt, Glenn. "Studying the CIA: An Agenda for Research." *Conflict Quarterly* 4, no. 3 (Summer 1984): 21-38.
95. Hastedt, Glenn. "The New Context of Intelligence Estimating: Politicisation or Publicising?" In *Intelligence and Intelligence Policy in a Democratic Society*, edited by Stephen J. Cimbala, 47-68. US: Transnational Publishers, 1987.
96. Hastedt, Glenn. "The Politics of Intelligence and the Politicization of Intelligence: The American Experience." *Intelligence and National Security* 28, no. 1 (2013): 5-31.

97. Hastedt, Glenn, and B. Douglas Skelley. "Intelligence in a Turbulent World: Insights from Organisational Theory?" In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 112-130. Abingdon: Routledge, 2009.
98. Hayden, Michael V. *The Assault on Intelligence: American National Security in an Age of Lies*. New York: Penguin Press, 2018.
99. Hayes, Darren R., and Francesco Cappa. "Open-Source Intelligence for Risk Assessment." *Business Horizons* 61 (2018): 689-97.
100. Hegemann, Hendrik. "Towards 'Normal' Politics? Security, Parliaments and the Politicisation of Intelligence Oversight in the German Bundestag." *British Journal of Politics and International Relations* 20, no. 1 (2018): 175-90.
101. Heymann, Hans. "Intelligence/Policy Relationships." In *Intelligence Policy & Process*, edited by Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle, 57-66. Colorado: Westview Press, 1985.
102. Hillebrand, Claudia, and R. Gerald Hughes. "The Quest for a Theory of Intelligence." In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael S. Goodman, 1-24. London: Palgrave Macmillan, 2017.
103. Hirsh, Michael. "US Intelligence Undercuts Trump's Case on Iran-al-Qaeda Links." *Foreign Policy*, June 24, 2019.
104. HM Government. *Online Harms White Paper*. London: APS Group, April 2019.
105. HM Government. *CONTEST: The United Kingdom's Strategy for Countering Terrorism*. London: APS Group, June 2018.
106. Holtmeyer, Dane. *The President and the Intelligence Community: The Importance of the Relationship – Fascinating Case Studies of John Kennedy, George H. W. Bush, and George W. Bush, Including Bay of Pigs, Desert Storm*. UK: Progressive Management Publications, 2018.
107. House of Commons: Public Administration and Constitutional Affairs Committee. *Lessons Still to be Learned From the Chilcot Inquiry*. March 16, 2017, HC656.
108. Hughbank, Richard J., and Don Githens. "Intelligence and its Role in Protecting Against Terrorism." *Journal of Strategic Security* 3, no. 1 (March 2010): 31-37.
109. Hulnick, Arthur S. "Relations Between Intelligence Producers and Policy Consumers: A New Way of Looking at an Old Problem." In *Intelligence and Intelligence Policy in a Democratic Society*, edited by Stephen J. Cimbala, 129-44. US: Transnational Publishers, 1987.

110. Intelligence Online. "DCRI, Hostage Negotiator." <https://www.intelligenceonline.com/government-intelligence/2010/04/08/dcric-hostage-negotiator,83192278-art>. Accessed July 11, 2019.
111. International Helsinki Federation for Human Rights. *Anti-terrorism Measures, Security and Human Rights*. Vienna: International Helsinki Federation for Human Rights, 2002.
112. *ITV*. "Prevent 'Not Trusted' by Many British Muslims and 'Must Reform'." February 19, 2017.
113. Jackson, Peter. Interview with David Chen. Personal Interview. Glasgow, March 21, 2019.
114. Jackson, Peter. "On Uncertainty and the Limits of Intelligence." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 452-771. Oxford: Oxford University Press, 2012.
115. Javid, Sajid. "Home Secretary Announces New Counter-Terrorism Strategy." Speech, London, June 4, 2018. Gov.uk. <https://www.gov.uk/government/speeches/home-secretary-announces-new-counter-terrorism-strategy>. Accessed July 11, 2019.
116. Jeffrey-Jones, Rhodri. *The CIA and American Democracy*. New Haven: Yale University Press, 2003.
117. Jervis, Robert. "Why Intelligence and Policymakers Clash." *Political Science Quarterly* 125, no. 2 (Summer 2010): 185-204.
118. Johnson, Loch K. "National Security Intelligence." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 3-32. Oxford: Oxford University Press, 2012.
119. Johnson, Loch K. "Sketches of a Theory for Strategic Intelligence." In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 33-53. Abingdon: Routledge, 2009.
120. Kahn, David. "A Historical Theory of Intelligence." In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 4-15. Abingdon: Routledge, 2009.
121. Kettl, Donald F. *Politics of the Administrative Process*. Thousand Oaks: CQ Press, 2017.
122. Kowalick, Phil, David Connery and Rick Sarre. "Intelligence-Sharing in the Context of Policing Transnational Serious and Organised Crime: A Note on Policy and Practice in an Australian Setting." *Police Practice and Research* 19, no. 6 (2018): 596-08.

123. Lambert, David E. "Addressing Challenges to Homeland Security Information Sharing in American Policing: Using Kotter's Leading Change Model." *Criminal Justice Policy Review* (2018): 1-29.
124. Laqueur, Walter. *World of Secrets: The Uses and Limits of Intelligence*. Somerset: Taylor & Francis, 1993.
125. Leadbetter, Wyland F., and Stephen J. Bury. "Prelude to Desert Storm: The Politicization of Intelligence." *International Journal of Intelligence and Counter Intelligence* 6, no. 1 (1993): 43-54.
126. Legrand, Tim. "'More Symbolic – More Political – Than Substantive': An Interview with James R. Clapper on the US Designation of Foreign Terrorist Organisations." *Terrorism and Political Violence* 30, no. 2 (2018): 356-72.
127. Levs, Josh, and Holly Yan. "Western Allies Reject ISIS Leader's Threats Against Their Civilians." *CNN*, September 23, 2014.
128. Lomas, Daniel W.B., and Christopher J. Murphy. *Intelligence and Espionage: Secrets and Spies*. London: Routledge: 2019.
129. Long, Austin G., and Joshua R. Shiffrin. "How Long Until Midnight? Intelligence-Policy Relations and the United States Response to the Israeli Nuclear Program, 1959-1985." *Journal of Strategic Studies* 42, no. 1 (2019): 55-90.
130. Lowenthal, Mark. *Intelligence: From Secrets to Policy*. Thousand Oaks: CQ Press, 2015.
131. Lowenthal, Mark. "The Policymaker-Intelligence Relationship." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 437-451. Oxford: Oxford University Press, 2012.
132. Lucas, Scott. "Recognising Politicisation: The CIA and the Path to the 2003 War in Iraq." *Intelligence and National Security* 26, no. 2-3 (2011): 203-27.
133. MacAskill, Ewen. "Spy Agencies 'Produced Flawed Information on Saddam's WMDs'." *Guardian*, March 12, 2019.
134. Macintyre, Ben. *The Spy and the Traitor*. Penguin: Milton Keynes, 2018.
135. Macrory, Sam. "Interview: David Anderson – Post-Brexit We Could End Up With Less Security Than We Need." *Prospect Magazine*, February 21, 2017.
136. Mandel, Robert. "Distortions in the Intelligence Decision-Making Process." In *Intelligence and Intelligence Policy in a Democratic Society*, edited by Stephen J. Cimbala, 69-84. US: Transnational Publishers, 1987.
137. Marrin, Stephen. "Evaluating Intelligence Theories. Current State of Play." *Intelligence and National Security* 33, no. 4 (2018): 479-90.

138. Marrin, Stephen. "Intelligence Analysis and Decision-Making: Methodological Challenges." In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 131-50. Abingdon: Routledge, 2009.
139. Marrin, Stephen. "Rethinking Analytical Politicization." *Intelligence and National Security* 28, no. 1 (2013): 32-54.
140. Marrin, Stephen. "Revisiting Intelligence and Policy: Problems With Politicization and Receptivity." *Intelligence and National Security* 28, no. 1 (2013): 1-4.
141. Marrin, Stephen. "Why Strategic Intelligence Analysis has Limited Influence on American Foreign Policy." *Intelligence and National Security* 32, no. 6 (2017): 725-42.
142. Mattis, Peter. "China Reorients Strategic Military Intelligence." *HIS Jane's*, March 3, 2017.
143. Miller, Greg. "Trump's Refusal to Pay Attention During Briefings Leaving Intelligence Officials 'Extraordinarily Frustrated'." *Independent*, December 13, 2018.
144. Mokhtar, Faris. "In the Fight Against Extremism, Singapore Needs to Ensure No Community Feels Marginalised: Shanmugam." *Today*, August 5, 2019.
145. Morrison, John N. L. "British Intelligence Failures in Iraq." *Intelligence and National Security* 26, no. 4 (2011): 509-520.
146. National Archives: Coroner's Inquest Into the Deaths of Diana, Princess of Wales, and Mr Dodi Al Fayed, February 20, 2008. https://webarchive.nationalarchives.gov.uk/20080521150227/http://www.scottbaker-inquests.gov.uk/hearing_transcripts/200208am.htm. Accessed July 11, 2019.
147. Negroponte, John D., and Edward M. Wittenstein. "Urgency, Opportunity, and Frustration: Implementing the Intelligence Reform and Terrorism Prevention Act of 2004." *Yale Law and Policy Review*. 28 (2010): 379-417.
148. Neo, Chai Chin. "Substantial Support for ISA in Singapore, Says Shanmugam." *Today*, August 5, 2019.
149. Nolte, William. "US Intelligence and its Future: Aligning With a New and Complex Environment." *Intelligence and National Security* 34, no. 4 (2019): 615-18.
150. Obama Barack, "Transcript of President Barack Obama's Remarks at CIA Headquarters." Speech, Langley, April 20, 2009. <https://www.cia.gov/news->

- information/speeches-testimony/president-obama-at-cia.html. Accessed July 12, 2019.
151. Office of the Director of National Intelligence. ODNI to Steven Aftergood, Washington DC, May 20, 2015.
 152. Office of National Intelligence. "Overview." <https://www.oni.gov.au/overview>. Accessed July 14, 2019.
 153. Olsen, Gorm Rye. "Transatlantic Cooperation on Terrorism and Islamist Radicalisation in Africa: The Franco-American Axis." *European Security* 27, no. 1 (2018): 41-57.
 154. Omand, David. "Creating Intelligence Communities." *Public Policy and Administration* 25, no. 1 (2010): 99-116.
 155. Omand, David. Interview with David Chen. Personal Interview. London, March 13, 2019.
 156. Omand, David. "Social Media Intelligence (Socmint)." In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael S. Goodman, 355-72. London: Palgrave Macmillan, 2017.
 157. Omand, David, Carl Miller, and Jamie Bartlett. "Towards the Discipline of Social Media Intelligence." In *Open Source Intelligence in the Twenty-First Century*, edited by Christopher Hobbs, Matthew Moran, and Daniel Salisbury, 24-43. New York: Palgrave Macmillan, 2014.
 158. Omand, David, Jamie Bartlett, and Carl Miller. *A Balance Between Security and Privacy Online Must be Struck*. Eindhoven, Demos: 2012.
 159. Omand, David, Jamie Bartlett, and Carl Miller. "Introducing Social Media Intelligence (Socmint)." *Intelligence and National Security* 27, no. 6 (2012): 801-23. <https://doi.org/10.1080/02684527.2012.716965>.
 160. Omand, David, and Mark Phythian. "Ethics and Intelligence: A Debate." *International Journal of Intelligence and Counterintelligence* 26, no. 1 (2013): 38-63.
 161. Palantir. "How a 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut." https://www.palantir.com/pt_media/how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut. Accessed July 11, 2019.
 162. Pascovich, Eyal. "The Devil's Advocate in Intelligence: The Israeli Experience." *Intelligence and National Security* (2018): 1-12.
 163. Pfaltzgraff, Robert L., Jr. "Intelligence, Deception and Surprise: Implications for the United States Policy in the 1980s." In *Intelligence Policy and National Security*, edited by Robert L. Pfaltzgraff Jr., Uri Ra'anana, and Warren Milberg, 297-314. Hong Kong: Macmillan, 1981.

164. Phythian, Mark. "Intelligence Theory and Theories of International Relations: Shared World or Separate Worlds?" In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 54-72. Abingdon: Routledge, 2009.
165. Pillar, Paul R. "Intelligence and US Foreign Policy: An Interview with CIA Veteran Paul Pillar." *Yale J. Int'l Aff.* (Summer 2013): 119-25.
166. Pillar, Paul R. "Intelligence, Policy and the War in Iraq." *Foreign Affairs* 85, no. 2 (March/April 2006).
167. Pillar, Paul R. "The Perils of Politicisation." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 472-84. Oxford: Oxford University Press, 2012.
168. Pinkus, Jonathan. "Intelligence and Public Diplomacy: The Changing Tide." *Journal of Strategic Security* 7, no. 1 (Spring 2014): 33-46.
169. Pitteloud, Jacques. "Terrorism, Counter-terrorism and Intelligence Studies: A New Industry?" *Journal of Policing, Intelligence and Counter Terrorism* 2, no. 2 (2007): 5-6.
170. Ransom, Harry Howe. "The Politicisation of Intelligence." In *Intelligence and Intelligence Policy in a Democratic Society*, edited by Stephen J. Cimbala, 25-46. US: Transnational Publishers, 1987.
171. Raufer, Xavier. Interview with David Chen. Personal Interview. Paris, June 19, 2019.
172. Richards, Julian. "Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy." *Intelligence and National Security* 27, no. 5 (2012): 761-80.
173. Roche, Edward. "Playing to the Edge: American Intelligence in the Age of Terror. By Michael Vincent Hayden. New York: Penguin Press, 2016." *Journal of Strategic Security* 9 no. 3 (Fall 2016): 106-08.
174. Rosenbach, Eric. "The Incisive Fight: Recommendation for Improving Counter-terrorism Intelligence." *Annals of the American Academy of Political and Social Science* 618, no. 1 (2008): 133-47.
175. Rovner, Joshua. "Intelligence-Policy Relations and the Problem of Politicisation." PhD diss., Massachusetts Institute of Technology, 2008, PhD in Political Science.
176. Rovner, Joshua. "Is Politicization Ever a Good Thing?" *Intelligence and National Security* 28, no. 1 (2013): 55-67.

177. Rubin, Michael. "The Temptation of Intelligence Politicisation to Support Diplomacy." *International Journal of Intelligence and Counterintelligence* 29, no. 1 (2016): 1-25.
178. Saggat, Shamit. "Boomerangs and Slingshots: Radical Islamism and Counter-Terrorism Strategy." *Journal of Ethnic and Migration Studies* 35, no. 3 (March 2009): 381-402.
179. Sampathkumar, Mythili. "Backlash Against Trump Grows as Almost 200 Former US Intelligence Officials Sign Letter Over Brennan Security Revocation." *Independent*, August 20, 2018.
180. Samuel, Henry. "Francois Hollande has Personally Authorised 'At Least 40' Targeted Killings Abroad, Says New Book." *Telegraph*, January 5, 2017.
181. Saner, Emine. "Former FBI Agent Ali Soufan: 'ISIS is not Over – It Will Take a Different Shape.'" *Guardian*, June 8, 2018.
182. Shaffer, Ryan. "Counter-Terrorism Intelligence, Policy and Theory Since 9/11." *Terrorism and Political Violence* 27, no. 2 (2015): 368-75.
183. Shamas, Diala. "A Nation of Informants: Reining in Post-9/11 Coercion of Intelligence Informants." *Brooklyn Law Review* 83, no. 4 (2018): 1175-226.
184. Sherlock, Ruth. "Taliban Members Released in Exchange for Bowe Bergdahl Begin New Lives in Qatar." *Telegraph*, June 7, 2014.
185. Simcox, Robin. "French Intelligence Reform." *Foreign Affairs*, July 17, 2016.
186. Simon, Joel. "The Business of Kidnapping: Inside the Secret World of Hostage Negotiation." *Guardian*, January 25, 2019.
187. Sims, Jennifer E. "Decision Advantage and the Nature of Intelligence Analysis." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 389-403. Oxford: Oxford University Press, 2012.
188. Snider, L. Britt. *The Agency and the Hill: CIA's Relationship with Congress, 1946-2004 – CIA Intelligence Papers*. UK: Progressive Management Publications, 2012.
189. Souris, Elena, and Spandana Singh. "Want to Deradicalise Terrorists? Treat Them Like Everyone Else." *Foreign Policy*, November 23, 2018.
190. *Spiegel Online*. "German Intelligence Service Negotiating Shalit's Release." August 29, 2009.
191. Staff, Pon. "Negotiation Analysis: The US, Taliban and the Bergdahl Exchange." Harvard Program on Negotiation Daily Blog. July 8, 2019. <https://www.pon.harvard.edu/daily/international-negotiation-daily/negotiation-analysis-the-us-taliban-and-the-bergdahl-exchange>. Accessed July 11, 2019.

192. Steinberg, Guido. "German Inefficiency." *Foreign Affairs*, January 19, 2017.
193. Stevenson, Jonathan. "Pragmatic Counter-Terrorism." *Survival* 43 no. 4 (2001): 35-48.
194. Tama, Jordan. *Terrorism and National Security Reform*. Cambridge: Cambridge University Press, 2011.
195. *Terrorism Legislation Reviewer*. "The Independent Reviewer's Role." <https://terrorismlegislationreviewer.independent.gov.uk>. Accessed June 28, 2019.
196. Thomas, Gordon. *Gideon's Spies: The Inside Story of Israel's Legendary Secret Service – The MOSSAD*. London: Aurum Press, 2014.
197. Thomas, Gordon. *Inside British Intelligence: 100 Years of MI5 and MI6*. London: JR Books, 2009.
198. Treverton, Gregory F. "Theory and Practice." *Intelligence and National Security* 33, no. 4 (2018): 472-78.
199. UK Home Office. "Counter-Terrorism and Border Security Act 2019: Designated Area Offence Fact Sheet." Counter-Terrorism and Border Security Act 2019: Factsheets. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778109/2019-02-11_Designated_Area_Offence_RA.pdf. Accessed June 28, 2019.
200. Warner, Michael. "Intelligence as Risk Shifting." In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 16-32. Abingdon: Routledge, 2009.
201. Webb, J. M. "Intelligence Theory: Key Questions and Debates." *Studies in Intelligence* 53, no. 2 (June 2009): 35-37.
202. White House. *National Strategy for Counterterrorism*. October, 2018. <https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf>. Accessed July 11, 2019.
203. Wicaksana, I Gede Wahyu. "The Consequence of Ethical Criticism of Intelligence on Countering Terrorism in Indonesia." *Asian Politics and Policy* 11, no. 1 (2019): 62-79.
204. Williamson, Lucy. "How France Hopes to Help Radicals Escape Jihadist Net." *BBC*, February 28, 2018.
205. Wirtz, James J. "The Sources and Methods of Intelligence Studies." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 59-69. Oxford: Oxford University Press, 2012.

206. Wirtz, James J. "Theory of Surprise." In *Intelligence Theory – Key Questions and Debates*, edited by Peter Gill, Stephen Marrin, and Mark Phythian, 73-86. Abingdon: Routledge, 2009.
207. Woodard, Nathan. "Tasting the Forbidden Fruit: Unlocking the Potential of Positive Politicization." *Intelligence and National Security* 28, no. 1 (2013): 91-108.
208. Younger, Alexander. "Fourth Generation Espionage – Fusing Traditional Human Skills With Innovation." Speech, St Andrews, December 3, 2018. <https://www.sis.gov.uk/news/alex-younger-st-andrews-speech.html>. Accessed July 11, 2019.
209. Zenko, Micah. "America's Virulent, Extremist Counterterrorism Ideology." *Foreign Policy*, May 21, 2015.
210. Zook, Chris. "The New Rules for Growing Outside Your Core Business." *Harvard Business Review*, May 4, 2015.