Conference Report

RUSI State Threats Taskforce: ‘Assessing the Responses’
192 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies.

© RUSI, 2023

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

## Contents

**RUSI State Threats Taskforce: ‘Assessing the Responses’**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Presentation: Key Findings from Workshop 1</td>
<td>2</td>
</tr>
<tr>
<td>Workshop 2: Further Reflections on State Threats</td>
<td>3</td>
</tr>
<tr>
<td>UK Government Architecture</td>
<td>5</td>
</tr>
<tr>
<td>Cyber Security and Information Operations</td>
<td>11</td>
</tr>
<tr>
<td>Illicit Finance</td>
<td>17</td>
</tr>
<tr>
<td>Conclusion</td>
<td>21</td>
</tr>
</tbody>
</table>
RUSI State Threats Taskforce: ‘Assessing the Responses’

Introduction

In line with the UK’s Integrated Review of Security, Defence, Development and Foreign Policy, RUSI set up a State Threats Taskforce to support the UK and its partners in detecting, understanding and responding to such challenges in February 2023. As part of this work, RUSI has held two expert workshops on different aspects of state threats. This report provides an overview of the key themes discussed in the second workshop in May 2023, which focused on the challenges faced by the UK national security architecture in responding to state threats, and potential approaches and actions which might improve the UK’s response.

The meeting opened with introductions and guidance from the chair, and an initial presentation recapping the findings of the first workshop, held on 9 February 2023. The presentation was used to frame discussions during the opening plenary session, which was followed by three parallel breakout group discussions looking at key challenges and recommendations for policy responses in the areas of central government, cyber security and information operations, and illicit finance. The meeting was concluded with a further plenary session to sum up key findings. As the meeting was conducted under the Chatham House Rule, names and affiliations of participants are not included here. For ease of reference, this report does not provide a direct transcript of the discussions, but an overview of participants’ insights, grouped by theme.

Presentation: Key Findings from Workshop 1

The opening presentation explored the current UK government understanding of state threats, defined as hostile acts, short of war, undertaken by state actors or proxies against the interests of the UK and its allies.³ It noted that the UK government envisaged 15 types of state threat combining vectors of attack and targeted assets grouped into five categories: threats to people; threats to assets and services; information acquisition; interference; and efforts to shape the international environment. The presentation noted several key findings from the first workshop:

• **Critique of the UK approach:** Participants had raised general concerns about the ambiguity of the definition of ‘state threats’, the comprehensiveness of the range of threats identified, and an apparent lack of prioritisation.

• **State actors:** Participants had noted four primary state actors of concern – Russia, China, Iran and North Korea – which used state agencies and proxies to undertake hostile and/or damaging acts. A number of other states loosely associated with these powers – for example, Syria, Venezuela and Cuba – were also highlighted, as were a number of other less obvious states, such as South Africa. However, it had been observed that levels of hostility, character of intent and capability varied widely. Participants had also noted the potential for damaging, if not explicitly hostile, activity by ‘non-aligned’ states such as India and Brazil, or even friendly states, such as Israel, especially in the development and deployment of cyber capabilities. Overall, there had been a perception that the problem of ‘state threats’ was not simply a clearcut contest between democracies and authoritarian states.

• **Vectors of attack:** Participants had noted the growing importance of cyber activity, including disruptive cyber operations and information operations, as vectors of attack in their own right and as enablers of other types of attack and campaigns of wider activity. There had been a strong emphasis on the role of criminal proxies in executing state cyber activities, affording them state protection to undertake other forms of criminality such as fraud, theft and ransomware attacks. A further area of concern had been the use of illicit finance as an enabler of political corruption and interference, and as a corrosive force on UK economic security.

• **Targeted assets:** Participants had confirmed the ongoing importance of the physical safety and security of UK citizens and residents, and the need to

---

protect domestic critical national infrastructure, although it had been emphasised that this needed to be considered from an international perspective in light of UK dependence on global supply chains and undersea infrastructure, such as the telecoms cables in Irish coastal waters, or shared UK/European energy lines.

Most significantly, however, workshop participants had expressed concerns about the detrimental effect of hostile/and or damaging state activity on political elites and democratic, legal, economic and social processes and cohesion.

- **UK resilience and capabilities**: Participants in the first workshop had assessed that the UK continued to enjoy significant resilience to state threats, in part as a result of active responses to ongoing strategic challenges such as terrorism, cybercrime, and serious and organised crime. UK intelligence and law enforcement agencies were highly competent and experienced, and structures existed within the UK government to coordinate an effective response, but there had been a concern that the exigencies of the Covid-19 pandemic, the war in Ukraine and subsequent economic instability had degraded some of these capabilities and reduced available resources. There had been further concerns about the level of energy, priority and coordination being devoted to state threats in the UK government compared with other security concerns.

In light of these discussions, several key themes emerged as areas for potential response, including: strengthening and coordinating centres in UK government tasked with tackling state threats; dealing with the challenge of political corruption through increased transparency; and developing a wider range of domestic and international partnerships.

### Workshop 2: Further Reflections on State Threats

Throughout the second workshop, participants provided further reflections on the threat-related concerns of the first workshop. One of the most persistent issues was how the term ‘state threats’ was to be defined, and whether that should be in a narrow sense, comprising only intentionally hostile acts by state actors or proxies, or more broadly, to include damaging, if not explicitly hostile, activities.

Although there was no settled consensus on this point, the weight of opinion in the workshop suggested that the current challenge posed by state threats was less clear-cut than during the Cold War. Primarily, there were concerns about
potentially ‘over-interpreting’ or misreading some states’ actions. While China, Russia and other states undertake hostile acts against the UK and its allies, many of these (espionage, for example) are within the boundaries of acknowledged activity that all states undertake, while some, although damaging to Western interests, are not necessarily intended to be hostile per se, either reflecting the pursuit of a domestic agenda or attempting to reshape international norms. In addition, several participants noted that larger and more capable states of concern such as Russia were chaotic and disorganised in conducting hostile or damaging acts: there was ‘no master plan’ and very often no coherent design to their behaviour, according to one participant.

This perception of a more disorganised threat than during the Cold War was also emphasised with regard to the relations between states; participants did not perceive two distinct blocs, authoritarian and democratic, in dedicated combat with each other. Some coordination and material support between authoritarian states was evident; for example, the supply of North Korean munitions⁴ and Iranian drones⁵ to support the Russian war effort. There was also some cooperation and knowledge-sharing between authoritarian states in order to avoid Western countermeasures, for example, between Iran and Russia on how to avoid economic and financial sanctions.⁶ However, these activities did not necessarily amount to formal alliances. Many of those non-aligned states with authoritarian tendencies that have sympathies for the behaviour of Russia or Iran also want to maintain their links and good economic relationships with Western-oriented democratic capitalist states.

A further area of caution was the problem of attribution. Participants observed that while the UK might assess that certain states, or their proxies, might be behind certain actions, these would be difficult to prove based on the intelligence available (especially in the realm of cyber). In practical terms, all that could be seen was a hostile act and its impact, rather than its origin or intention. This meant that it would be difficult to develop responses that either disrupt or deter such attacks at source, although the UK Ministry of Defence (MoD) was beginning to make efforts to use AI to tackle this challenge in collaboration with the private sector.⁷

---

Given the diversity and ambiguity of the risks posed, whether in terms of origin, intention or coordination, the weight of opinion in the workshop emphasised the importance of the UK being able to develop resilience in the face of the most harmful state-inspired activity. Yet, several participants also stated that a generally defensive posture should not preclude the development and deployment of offensive capacity where the origin and intent of an attack was clearer and its significance more pronounced. Nor should it limit proactive work in the diplomatic sphere to shape the international environment. As several participants noted, although it was important to be able to withstand attacks or damaging activity, this had to be balanced against actions taken to reduce the chances of such attacks occurring in the longer term.

The following three sections focus on the three parallel breakout room discussions.

**UK Government Architecture**

Participants noted that as external observers of the UK government, it was difficult to fully understand the organisation of the response to state threats on the basis of the policy statements that had so far been released, or through their own ongoing contacts with government.

However, participants acknowledged a wide range of departmental and agency activity – policy focused, analytical and operational – targeted at different aspects of state threats. Various departments, for example the Cabinet Office, Foreign, Commonwealth and Development Office (FCDO) and the MoD, were understood to have units focused on developing relevant policy, with the Homeland Security Group at the Home Office holding policy oversight. The Joint State Threats Assessment Team (JSTAT), based at the Security Service, provides all-source intelligence assessments on state threats, feeding these into the Joint Intelligence Organisation (JIO) at the Cabinet Office, alongside existing intelligence streams from the agencies. The UK intelligence community itself has also long been tackling hostile state activity at home and overseas, both offensively and defensively, while the National Crime Agency (NCA) has begun to play an increasingly significant role in combating overseas organised crime groups (OCGs) potentially linked to hostile regimes. On top of these layers of activity,

the National Security Council (NSC)\(^{11}\) and National Security Secretariat (NSS)\(^{12}\) provide a mechanism for coordinating and prioritising state threats, in theory at least.

Participants further noted that new elements have continued to be added to this infrastructure, such as the National Protective Security Authority (NPSA), which began work in spring 2023.\(^{13}\) Initiatives such as the National Preparedness Commission\(^{14}\) are also considering various risks relevant to state threats, such as UK preparedness in the event of a major incident or attack.

### Challenges: Coordination and Prioritisation

Although activity is taking place across the UK government, participants believed it was less clear that it was of significant magnitude, with sufficient resources or coordination, to support effective delivery. While departments have set up appropriately named state threats units, these still appear to be siloed from other similar units, creating overlaps, wasting resources and generating friction and competition. Workshop participants had no sense of who the ultimate risk owners for state threats might be, or which ministers and officials are accountable for success or failure. There were additional concerns that those departments that are risk owners in the state threats space – the Treasury, for example, in terms of illicit finance and economic security – do not see themselves as such.

Moreover, with the current imperatives to control public finances, participants judged that officials are being incentivised to restructure and rebrand existing work as ‘state threats’ to satisfy a requirement to show activity. As a result, public statements that claim to show the development of policy in the area tend to be communications pieces listing renamed activities, rather than explanations of intended outcomes and supporting strategies. Participants identified a variety of reasons for why this situation has occurred.

1. **Lack of political will and leadership:** Participants perceived an absence of political leadership and ambition in state threats. Several participants felt that senior ministers have not taken the issue seriously enough, in particular the potential for corruption of political elites, institutions and processes. There has been no strong push from the prime minister nor from an empowered senior cabinet minister to take the issue of state threats seriously and drive

---

coordinated action across departments, as happened with counterterrorism after 9/11. There are indications, several participants felt, that ministers wish to discuss state threats, but do not wish to pay for dealing with them.

2. Ambiguity and lack of a compelling narrative: Participants reiterated previous concerns that as yet the UK government’s approach is hampered by ambiguities on the concept of state threats. In the words of one participant, ‘it can mean everything, and it can mean nothing’. Whereas the mission in counterterrorism is clear – to stop terrorist attacks – the objectives and aims in tackling state threats are more diffuse and amorphous. Therefore, it is difficult to shape a narrative that would drive strategic action and encourage public support. In the words of another participant, the issue of state threats remains ‘below the line of public concern’, much in the same way that Islamist extremist terrorism did in the 1990s.

3. Commercial versus security concerns: Participants judged that ministerial unwillingness to take state threats seriously comes in part from an ethos which places commercial concerns above those of national security. The main target is making and saving money for ‘UK plc’. One participant highlighted a recent speech by Jake Sullivan, US national security advisor, which noted that the requirements of the neo-liberal economic philosophy undermined public goods, and therefore need to be addressed and rebalanced.15

4. Limited skills and resources: A further concern among members was an apparent weakening of the required skills, competencies and resources needed to tackle state threats within relevant UK departments and agencies. Several expressed fears that competence and capability are major problems, with not enough focus on the delivery of tangible objectives within and across departments.

5. Weakening of analysis and assessment: One area of particular concern for some participants was the weakening of the UK’s analytical and assessment capabilities, which hampers the government’s capacity to build a convincing intelligence picture around state threats. Despite the existence of JIO, JSTAT and other analytic teams, there was a perception that not enough resources are devoted to analytic effort. Many departments have small analytic capabilities, which are managed ‘off the side of the desk’, and JSTAT itself was seen as a ‘poor relation’ in comparison to the much larger Joint Terrorism Analysis Centre (JTAC).16 One participant noted that when new funds become available, they are ‘always much more likely to go to those who “do” over those


who “think”, leading to much analysis being outsourced to academia. A linked concern was an absence of effective knowledge-management systems and processes on state threats issues both within departments and across UK government.

Responses: Enhancing Political Will

Participants argued that a step-change in attitude is required to tackle the state threats issue, and to ensure that the UK government architecture is agile and sufficiently well resourced to do so. There was near universal agreement that political leadership needs to take the issue of state threats more seriously than has been the case. At the same time, there was a recognition that political will cannot be conjured from thin air in the absence of a major crisis – ‘the political earthquake effect’ – and that responsible officials within government, in dialogue with civil society, need to develop a case that combines a political ‘want’ – to tackle state threats – with a set of political ‘cans’, or actions, that would then lead to a political ‘must’.

There was no settled view from the workshop participants on how this might happen, but several noted how cyber security had become a greater issue once senior officials ‘signalled’ the importance of the issue from within government to the public via the media and wider civil society engagement, engendering the creation of the National Cyber Security Centre (NCSC) in 2016.

Others suggested that the public could be engaged through highlighting the risks that state threats, especially external influence and corruption, could play in undermining democracy, a core dimension of UK life highly valued by its citizens. The issue must be felt as a real risk and concern to the lives and livelihoods of individuals and families. A further suggestion was to frame the issue as one where the UK could play an international lead, especially in the Five Eyes community and NATO, which is likely to appeal to ministers as well as the public.

Responses: Strengthening the Centre

On the assumption that necessary political will would grow over time, participants suggested areas of activity where the UK government could improve its response:


1. **Tackling corruption risks:** One of the areas of strongest consensus was the need for the UK’s political leadership to take the issue of state threats seriously, especially with regard to the potential corruption of the political process and the undermining of institutions. There was wide support for greater transparency on the receipt of overseas funding by members of both Houses of Parliament, as well as political parties, think tanks and media outlets. A further suggestion was a refresh of the Nolan Principles\(^\text{19}\) on conduct in public life, encouraging all political parties to endorse and support them publicly. Such a refresh would need to highlight the role they play as a barrier to negative external influence, and thus the importance of the Principles to UK national security.

2. **Developing definitions, assessments and strategy:** As previously discussed, participants agreed that much greater effort was required to clarify the meaning of the term ‘state threats’, to develop a tailored intelligence picture and map threats and vulnerabilities. These policy elements could then be used to prioritise the harms arising to the UK and its interests, identify risk owners and actions, and structure a cross-government response. Several suggested the utility of the UK Counter-Terrorism Strategy’s (CONTEST) ‘four Ps framework’ (Pursue, Prevent, Protect and Prepare),\(^\text{20}\) which created a clear and understandable framework for counterterrorism in the early 2000s. Participants also stressed that using a similar, if not identical, framework would help frame a public strategy that could be shared and internalised by the private sector, civil society and the public.

3. **Re-energising existing governance structures:** The majority of participants believed that the governance structures necessary to coordinate and prioritise responses to state threats already exist, especially in the Cabinet Office (the NSS and JIO were mentioned by several). It was important therefore not to create new departments and organisations as a substitute for making the current machinery work as intended, as unnecessary changes could prove disruptive. However, several others suggested the need to create a dedicated state threats unit, either in the Cabinet Office or another major department such as the Home Office or FCDO, to help focus and coordinate efforts. Whichever approach is taken, it was agreed that there needs to be a clear and precise recognition of risk ownership and accountability at strategic, operational and tactical levels.

---


4. **Enhancing institutions and resources**: There was a common perspective that institutions tackling state threats need to be better resourced to underpin effective action. One area where there was an interest in seeing an uptick in investment was analysis and assessment, with JSTAT and relevant departmental teams being better staffed. As a complement, not an alternative, to an improvement in resources, it was also suggested that analytic functions should develop deeper connections with the wider research and policy communities looking at state threats outside government.

5. **Applying a ‘whole-of-government’ approach**: Participants observed that while it was probably unnecessary to bring radical change to UK government infrastructure, it is also vital to ensure that all relevant departments and agencies are included at an appropriate level in the crafting and delivering of the state threats response. The role of the Treasury as a risk owner around illicit finance was emphasised by several, as well as the Department for Culture, Media and Sport (DCMS) and the Department for Science, Innovation and Technology (DSIT) around cyber and information risks. Other workshop members noted the importance of ensuring that NCA activities against OCGs are fully integrated with relevant operational streams of the intelligence agencies and the military.

6. **Addressing the commerce versus security paradox**: Several participants suggested that the current implicit hierarchy of concerns in UK government philosophy needs to be addressed. While there was no appetite for the ‘securitisation’ of UK economic, finance or cultural policies, it was felt that there needs to be an explicit acknowledgement that many activities fundamental to an open society are open to abuse from outside, and that when policy decisions are made, the ‘security angle’ must be considered. It was seen as particularly vital that the Treasury sees itself not only as a promoter of UK prosperity, but also as a guarantor of its economic and financial security.

7. **Focusing on resilience but being proactive**: A recognition of the complexity of the threat, and especially the difficulties posed by understanding the origin and intention of attacks or damaging acts, meant that the primary focus of a state threats response has to be on resilience. Nonetheless, several participants noted that to take a purely defensive posture would not provide any deterrent or punishment, potentially incentivising ongoing hostile or damaging activity. Where intention and origin can be more confidently detected, therefore, the UK needs to ensure it is prepared to take active measures in response. Again, however, such responses would need to be considered within the bounds of what overall international norms and standards of behaviour the UK wishes to encourage. While not constraining the UK government too far, the potential unintended consequences of an excessively offensive response to state threats needs to be factored in.
8. **Adopting a ‘whole-of-society’ approach:** In tandem with the need for a ‘whole-of-government’ approach, participants stressed the importance of private sector, civil society and public engagement. There was interest in the potential application of the Swedish ‘Total Defence’ model, which encourages businesses, institutions and individuals to take up responsibility for societal defence in partnership with state agencies. Several participants noted synergies here with the development of the NCSC, which led to an open dialogue with the private and public sectors about cyber security, and the development of the Joint Money Laundering Intelligence Taskforce (JMLIT), which has enabled a new intelligence-sharing channel between law enforcement and the financial services sector. One participant suggested the National Security Communications Team at the Cabinet Office could play a leading role in developing a narrative to generate public support.

**Cyber Security and Information Operations**

Participants noted that cyber security and information operations were discrete topics, the former dealing with intrusions into a network or system to cause disruption and the latter the use of cyberspace for psychological operations, such as disrupting society or influencing elections. As a result, they needed to be treated separately.

**Challenges: Cyber Security**

The perception of workshop participants was that the UK is a global leader in terms of cyber, with a strong narrative of action over the past 30 years. In what one participant described as a ‘three-stage journey’, the UK has gone from taking the ‘pain without response’ in the 2000s to developing a robust strategy and infrastructure in the 2010s to a more flexible and agile response in the 2020s. Several participants emphasised the important role of the NCSC as a central hub of operational activity against cyber-linked state threats, a leader of public

---


dialogue, and a key player in policy coordination with the NSC, the Government Security Group and DSIT. Within the decision-making infrastructures linking these stakeholders, it was assessed that a clear risk ownership and a functional system for prioritisation of cyber security risks exists.

Participants noted that the private sector is also deeply involved in cyber security partnerships through the NCSC Industry 100 scheme (i100),\(^\text{24}\) which supports secondments from the private sector into NCSC, and the Cyber Security Information Sharing Partnership (CiSP),\(^\text{25}\) designed to facilitate real-time intelligence sharing between the public and private sectors. The UK government has also sought to drive up cyber security standards in the private sector and civil society through direct advice and awareness campaigns such as NCSC’s Cyber Aware, and the NPSA’s Security Campaigns.\(^\text{26}\) It has sought to stimulate a more agile, risk-based approach to communications network resilience with a new regulatory framework set out in the Telecommunications (Security) Act (TSA), which came into force on 1 October 2022.\(^\text{27}\) The UK has also played a major role in ongoing international discussions on cyber security standards, and developed world-leading cyber security frameworks, such as the Bank of England’s CBEST threat simulation methodology.\(^\text{28}\)

Despite the overall positive assessment on cyber security, however, some participants saw a risk of becoming complacent, with one noting that the UK’s cyber security, while strong so far, is entering a ‘troubling adolescent phase’. Participants were particularly concerned about the scale and depth of available public sector resources, especially for investigations. As one noted, ‘the problem is large and not enough people are involved in the response’. There was a risk, therefore, that some lower prioritised risks – potentially including less obvious state threats – might fall off the operational agenda.

There were concerns too that some aspects of cyber security are not as well managed as others. Some noted that cyber-related threats can sometimes be treated in isolation from other vectors of attack, hampering the effectiveness of response. A major concern – voiced by several participants – was that the response to cybercrimes such as fraud are not well integrated into the wider cyber response,

---


given that OCGs linked to hostile state actors are likely to be a part of that threat. It was also felt that local police forces do not have the same level of awareness or private sector engagement as national agencies. In addition, some believed that offensive cyber operations are neither as well resourced nor coordinated as defensive preparation and incident response.

Challenges: Information Operations

Participants noted that the publicly available material on the UK’s management of information operations is more limited than for cyber security, although there are several indications of growing activity. In 2018, the MoD created the National Security Communications Unit to counter external information operations but further details have not been reported in Parliament or the media. In February 2019, the House of Commons Committee on Digital, Culture, Media and Sport published its report on disinformation and fake news, which provides recommendations for enhanced private sector responsibilities for tackling disinformation, although these have yet to be actioned by the government. Action has also occurred in the development of offensive information operations; in February 2023, the UK government published ‘Allied Joint Doctrine for Information Operations’, recently agreed across NATO, which provides practical guidance for the conduct of information operations. Alongside these public sector initiatives, the government has also been seeking to pass the Online Safety Bill, which would require social media companies to protect children and adults online and features specific powers to deal with terrorist content. Participants suggested that UK government departments and agencies are also working with major social media platforms on information operations on a case-by-case basis.

Nonetheless, the consensus view of workshop participants was that the UK’s response to information operations is well behind that of cyber security. Based on what participants knew, there is limited coordination on information operations across agencies and departments, and engagement with the private sector is much less mature than for cyber security. One of the suggested reasons for this more limited response is the difficulty of measuring impact, disruption and costs from information operations in comparison with cyber attacks, where it is thus easier to encourage private sector involvement.

Responses: Public Sector

In light of the broadly supportive assessment of the UK government’s approach to cyber security, the main emphasis of participants was on maintaining the continuity of the current model, which comprises strong government-led coordination and private sector engagement. The creation of a new public institution to tackle cyber, a so-called ‘NHS of Cyber’, was deemed unnecessary. However, some changes were suggested, including the consolidation of the police response to cybercrime into a unit operating at national level, which would enable its better coordination and integration with other cyber security threats. The UK also still has room to learn from the experiences of overseas partners, especially in the testing of cyber threat simulation methodologies such as the EU’s Threat Intelligence-Based Ethical Red Teaming (TIBER), Australia’s Cyber Operational Resilience Intelligence-Led Exercises (CORIE), Hong Kong’s Intelligence-led Cyber Attack Simulation Testing (iCAST) and Singapore’s Adversarial Attack Simulation Exercises (AASE).32

Participants also wished to see a much stronger UK response to information operations underpinned by a clear public strategy and coordination by a lead department such as the Home Office or DSIT, with involvement of the Information Commissioner’s Office and Advertising Standards Agency and NSC oversight. Several suggested the need to widen legalisation to support this, including through an update to the Online Safety Bill that would incorporate challenges around state actor-inspired misinformation.

Participants also showed some interest in exploring the possibility of more proactive measures to deter bad actors in cyberspace. Some were supportive of a US-style approach which would ‘name and shame’ bad actors, and the use of targeted financial sanctions and no-fly bans against state-linked cyber criminals. However, others believed that these efforts were likely to be punitive at best and would likely prompt retaliatory measures against those working in cyber at UK agencies.

Responses: Private Sector and Civil Society

Participants saw the private sector as a vital element in the UK’s ongoing response to cyber threats and information operations. On cyber security, there was a wish to see a continuity of approach, with the government mandating standards of cyber resilience through legislation and regulation, direct engagement in knowledge and intelligence sharing, and shared capacity-building efforts. Several participants believed these efforts could be developed further with reform of the 1990 Computer Misuse Act to re-target efforts on issues such as fraud and other economic crimes, enhance intelligence-sharing and enable private sector firms to ‘hack-back’ against those seeking to penetrate and disrupt their systems – already allowed under US law. Some participants further suggested that private sector firms could be encouraged to take out cyber security insurance to protect them from the potential of a major attack. Nonetheless, although participants wished to see the private sector playing a significant burden-sharing role, it was felt that this should not be used as an excuse for public sector agencies to pull back, which could leave gaps in areas where multiple smaller firms had fewer resources, or larger firms saw less of a financial or regulatory requirement to act.

On information operations, by contrast, participants believed that a greater UK government effort is needed to drive action from technology and social media firms on state threats without the need for legislation or regulation. Suggestions included encouraging the development of a state threats-focused industry partnership similar to the Global Internet Forum to Counter Terrorism, founded in 2017 to tackle extremist online content by firms including Microsoft and Facebook, or the promotion of a code of practice along the lines of the International Association of Business Communicators Code of Ethics, which stresses a responsibility to communicate accurate information. Several participants pointed to EU initiatives such as the Code of Practice on Disinformation as a potential model for a voluntary code which would place greater onus on platforms to deter, detect and disrupt misinformation.

However, participants also accepted that whereas the lack of commercial incentives for firms to work closely with government on information operations needs to be addressed, the UK government could not expect technology and social media firms to fall into line, and efforts would be required to develop a

business case to encourage their involvement, possibly involving close cooperation on intelligence sharing, investigative coordination and capacity-building. If this did not prove effective, further consideration of legislative and regulatory changes, including potential penalties and enforcement, might be required.

Participants also noted that academia, civil society and the public should be involved in deterring and disrupting information operations. Non-UK initiatives highlighted as potential models that could be emulated included the recently announced European External Action Service’s Information Sharing and Analysis Center, which has developed a platform for sharing information on the spread of online disinformation, and the Finnish digital literacy journey, which trains students to apply critical thinking to online media stories and social media trolls.

Responses: International Partnership

Participants also emphasised the need for UK actions to be taken in collaboration with international partners in the Five Eyes community, Europe and beyond. A joint statement by Five Eyes members with Germany and the Netherlands in April 2023, encouraging the private sector to build technology secure by design and default, was noted as a positive example of how the UK could play a role in helping set common standards on cyber security. Another area of proposed collaboration was on overseas cyber capacity-building in areas targeted by Russia and China such as Eastern Europe, East Asia and Southeast Asia. Although there was an expectation that this would require some UK public funding, it was noted that major UK businesses with relevant overseas interests could be encouraged to lead by example. Participants did not see any grounds for cooperation or agreement of standards with potentially hostile actors, and it was also assessed that collaboration with major non-aligned powers such as India remains unlikely for now, given their desire to maintain good geopolitical and economic relationships with some anti-Western states. However, dialogue should continue.

---


Illicit Finance

Participants noted that the UK has a well-developed framework for tackling different dimensions of illicit finance. As a member of the Financial Action Task Force (FATF), the UK is a leading voice in the promulgation of the FATF’s 40 Recommendations, a set of minimum standards in the fights against money laundering, terrorist financing and proliferation finance. The Recommendations place obligations on the financial and other regulated sectors to undertake customer due diligence and issue suspicious activity reports to a national financial intelligence unit (FIU) as preventative measures against financial crime. In the UK, the execution of these obligations is overseen by a range of regulatory bodies, the most important of which is the Financial Conduct Authority. The primary national law enforcement agency with competence for financial crime is the NCA, which also houses the UK’s FIU. The UK also has a public–private partnership on financial crime, the JMLIT, founded in 2015, and its own autonomous national sanctions regime underpinned by a range of legislation including the Sanctions and Anti-Money Laundering Act 2018.

Challenges: No ‘Business Case’

Participants noted that while the issue of state threats was touched on by several aspects of the UK’s anti-financial crime regime, the relationship is only implicit. The FATF Recommendations and relevant UK laws and regulations do not explicitly foresee the potential abuse of illicit finance in support of hostile state activity, and therefore regulators and law enforcement have paid the issue little attention. In parallel, public agencies have a weak understanding of the financial dimensions of state threats, and lack sufficient expertise, resources or will to rectify this situation.

Given the absent regulatory obligations around illicit finance and state threats, the private sector is thus largely focused on those areas where it is most at risk of regulatory enforcement action, such as sanctions evasion, and to a lesser extent, the laundering of the proceeds of bribery and corruption. Even in this latter case, however, corruption is seen more through the lens of corrupt kleptocrats using the UK as a home or conduit for their proceeds of crime than as a potential threat to the UK body politic. When firms are required to identify

politically exposed persons (PEPs) during customer due diligence, they are expected to do so to clarify financial crime risks rather than identify malign state influences. Concerns about the impact on national economic security of overseas investments from high-risk jurisdictions are also not considered, as this is not an area where UK financial institutions have any significant legal obligations.

Alongside the lack of regulatory imperatives, participants assessed that the private sector does not feel direct moral pressure from the UK government, regulators or agencies to take action on illicit finance linked to state threats. To the extent that there is any interest in the issue, the messages emanating from different parts of the UK public sector were seen as discordant and episodic. Although cases with state threat dimensions have been covered in public–private dialogues, they are not presented as ongoing shared threats, and from the perspective of the private sector, the UK government’s behaviour seemed inconsistent; the willingness of the UK government to allow Yevgeny Prigozhin, head of the Russian paramilitary Wagner Group, to mount a libel action in the UK while subject to UK sanctions was noted by several.41 As a consequence, the private sector took the view, in the words of one participant, ‘if the government doesn’t seem to care … why should we?’.

In fact, several participants noted that there were significant disincentives to take action, not least of which would be shutting down commercial opportunities and generating additional costs to monitor and investigate state threats. A further layer of complexity for international financial institutions would be the potential for conflicts of interest in overseas markets which might be areas of concern for the UK government. For some of the larger banks, this would clearly be a constraint in eastern Europe, the Middle East and East Asia. A further barrier to financial institutions taking proactive measures on state threats was also the fear that by taking action they would make themselves regulatory targets as they would be creating a new risk for which they might suffer enforcement action. As a participant noted, the current regime in the UK encouraged regulators to look less at bad actors and more at the intermediaries who could be more easily punished for failure to prevent illicit activities.

A final concern was that, even if financial institutions were prepared or required to take up the issue of state threats, they themselves present a new vulnerability because of the susceptibility to insider threats. Not only could compromised bank staff provide a valuable conduit for information gathering by overseas intelligence services, but they could also offer the potential to exert influence on UK economic and financial policymaking. Even without direct private sector

access to secret intelligence, there are already anxieties about the private sector acting as the ‘soft underbelly’ or ‘backdoor’ for malign activity; for example, one participant expressed concerns about the NCA's decision to share typological and strategic intelligence openly with the private sector on Russian sanctions evasion techniques in 2022, which they judged could be used by evaders to work around any new countermeasures.

Responses: Obligations and Incentives

There was wide agreement among participants in the workshop that the UK government must find ways to engage the regulated private sector in the management of state threat risks linked to illicit finance, but without causing serious disruption to financial stability. There was some interest in clarifying and extending legislation to create new obligations on illicit finance linked to state threats: one suggestion was to identify trading in influence as a predicate financial crime offence. But overall, there appeared to be little appetite for imposing significant new legal and regulatory obligations. Nor was there a desire to see the UK financial sector securitised to the extent that it has material effects on private sector profitability. Therefore, participants wished to see the private sector incentivised rather than forced to engage on state threats. Several approaches to achieving this were discussed:

- **Clarifying and unifying UK government engagement:** Even under the current regulatory and law enforcement agency arrangements, there was a perception among participants that the UK government and its agencies speak to the regulated private sector in many conflicting voices, even via shared mechanisms such as the JMLIT. Dialogue on financial crime and security risks would thus benefit from a more unified, coordinated and consistent UK government approach and narrative. Participants also felt that, on the specific issue of state threats, engagement would also benefit from more consistent and wholehearted involvement of the UK intelligence agencies.

- **Articulating a narrative around reputation and responsibility:** Several participants noted that there have already been conversations between the UK government and the financial services sector which led to the latter’s active involvement in tackling issues such as human trafficking and the illegal wildlife trade, based more on reputational risks, ethical concerns and wider corporate social responsibility, than immediate commercial imperatives. Others noted that the private sector is likely to respond if it is clear that state

---

threats are a national priority, or a wider concern of leading Western economies. However, it was also agreed that costs and benefits could not be ignored and that the UK government would need to ‘incentivise the upside’, perhaps by stressing the value of gaining insights from engagement or creating moral capital with regulators, while ‘de-risking the downside’, by noting the long-term potential effects of declining reputation on share price, or the future risk of regulatory change if voluntary actions were not taken, or the wider impact on the UK’s reputation and credit ratings.

- **Clarifying risk appetite and providing guidance:** Because of the potential tensions between commercial concerns and the economic and financial security agendas, participants observed that the government would also have to provide a sense of risk appetite and ‘red lines’ to drive business-level action, underpinned by clear guidance on how to engage with potential transactions and relationships where there might be national security sensitivities. Such guidance would need to make it apparent that government does not wish to prevent commercial ties with less friendly countries per se, but only stop hostile state actors from abusing the financial system for malign reasons. One suggested area where the government could introduce relevant private sector guidance quickly was the management of so-called ‘insider risks’, where employees and/or former employees use access or knowledge to damage an organisation.

- **Using existing machinery for cooperation:** Participants stressed that engagement with the regulated private sector on state threats needs to be an ‘official conversation’, and not conducted surreptitiously or as a bilateral informal discussion between businesses and UK government agencies. Several noted that JMLIT could provide a framework for such a conversation, although it was accepted that its remit, structures and membership would need to be extended to enable effective and sustained cooperation. Processes and procedures would need to be put in place to allow the sharing of appropriately classified assessments and intelligence with the private sector, emphasising the need for the UK government to reform current vetting channels for private sector staff. Correspondingly, both public and private agencies would need to review the security and efficiency of current processes for sharing financial data.

- **Starting with a pilot project:** Participants agreed that to get substantive engagement moving once the right enablers were in place, JMLIT or any alternative mechanism would need to start with discrete areas of well-defined cooperation to prove the concept. An area suggested, based on the concerns of many participants in the workshop, was to look at the flow of illicit overseas

---

funds into the UK political process. It was judged that this would be one touch point where there would be genuine synergy between intelligence and assessment available to agencies with the data and financial analysis open to the private sector. It was further suggested that academia and think tanks might be involved in more strategic and less sensitive aspects of this dialogue, potentially helping to provide context and assessment of the shared intelligence.

While participants expressed broad support for closer collaboration between the public and private sectors on illicit finance linked to state threats, several also noted that it was important to consider the potential unintended consequences of action. Several participants believed it was vital that the focus remained on the bad actors rather than the financial services sector itself. If this did not occur, there were concerns that the sector would become more guarded in how it engaged. In addition, there were concerns that a public recognition of improved collaboration might drive illicit activities into less well-resourced areas of the private sector, forcing the need for public sector engagement with a much wider number of smaller businesses. This would bring its own challenges for sharing sensitive intelligence and assessments, necessitating the need to calibrate public exposure of levels of cooperation.

Conclusion

The discussion across the plenary sessions and breakout groups was diverse, and as several participants noted, could only tackle a limited number of aspects of the response to state threats. As one participant observed, the focus on issues such as cyber security and illicit finance tended to ignore more traditional vectors of hostile state activity, such as espionage via human sources, or the use of diaspora communities as tools of overseas state action. Nonetheless, given the current ubiquity of cyber and illicit finance as enablers of a variety of state threats, it was judged appropriate that they were prioritised in the short time available and indeed many of the discussions around these issues also had wider relevance to other potential vectors of attack.

At the conclusion of the second workshop, the chair and participants noted several persistent themes that had recurred across both workshops. And although not providing a detailed agenda for UK government action as yet, they did indicate the broad philosophical underpinning for future recommendations:

- **The need to clarify and understand the threat**: It remained unclear to many in the workshop how the UK government understands the term ‘state threats’, and as a result, official thinking remains ambiguous. Clarity is required, and, even if a narrow definition is chosen, the UK government needs to ensure
that other linked concerns, such as indirect and damaging state activity, also receive a suitable policy response.

- **The need to give security concerns their due.** Consequently, the UK government needs to re-evaluate its thinking about issues of national security and the potential vulnerabilities of an open society. In the years since the end of the Cold War, the UK has increasingly prioritised commerciality over security. While there was no appetite in the workshop to see the country become a ‘garrison state’, it was agreed that security concerns require greater weight in policy- and decision-making.

- **The need to face up to the risk to democracy:** As part of this reassessment of attitudes, it was further agreed that the UK needs to confront the potential risk to its democracy and open society, if sustained action is not taken soon. There was a persistent anxiety across the workshops that UK processes and institutions are being slowly corroded by malign and damaging external influences, intentional and otherwise, and that this has to be addressed urgently.

- **The need for coherent and sustained action in government:** All participants concurred that this clearer view of the threat and potential dangers to the UK necessitates a more coherent, coordinated and sustained approach from the UK government. In no area was there a sense that this required radical reform of most of the machinery or institutions of government, but rather an infusion of energy and purpose, and the better integration of some areas of activity (for example, cybercrime and information operations) into the overall UK approach. High-level political will and buy-in are essential.

- **The need to communicate the threat with clarity and consistency:** The nature of the threat and the harms faced by the UK need to be articulated clearly and consistently to the private sector, civil society and the public. At present, there is still a mood outside government that state threats are happening elsewhere, and that the UK is insulated from these issues by virtue of geography. However, while not seeking to generate panic, UK citizens need to be disabused of this view by sober public messaging similar to that used in Scandinavian countries.

- **The need to engage beyond government:** Workshop members recognised that although the UK government will have to take the lead in tackling state threats, it will not be able to do so without wider societal engagement. Businesses, civil society institutions and the public will need to be encouraged, incentivised and, in some instances, obliged to respond constructively to the new public messaging.

- **The need to take a consistent international approach.** Participants noted that while some of the issues facing the UK are distinct, most are also being faced by friends and allies. The UK should therefore not seek to act alone and should engage in cooperative dialogues with partners in the Five Eyes...
community, Europe and beyond. These dialogues should look not only toward direct cooperation, shared standards and, where appropriate, burden-sharing, but also to pool knowledge and best practice where states have developed effective responses. Regardless of the difficult geopolitical environment, moreover, participants stressed that the UK should continue to engage with a wide range of non-aligned states on these issues, seeking to encourage compliance with accepted international standards, even in discouraging circumstances.