Conference Report

RUSI State Threats Taskforce: ‘Assessing the Threats’
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, 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.

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/>.

RUSI State Threats Taskforce: ‘Assessing the Threats’

Introduction

In line with the UK’s Integrated Review of Security, Defence, Development and Foreign Policy (IR), RUSI has set up a Taskforce on State Threats, to support the UK and its partners’ ability to detect, understand, attribute and act in response to such threats. As part of this work, the RUSI team is conducting two expert workshops on different aspects of state threats. The following meeting note provides an overview of the key themes discussed in the first workshop, held online on 9 February 2023, which focused on: state threat actors, vectors and targets of attack; vulnerabilities; and strengths and weaknesses in UK capabilities.

The meeting was structured around an opening plenary discussion, with an initial presentation that outlined the evolving UK government approach to state threats. The presentation noted that the UK government has identified state threats as overt or covert actions orchestrated by a foreign government which fall short of war, and which contain three elements: a state actor; a vector of attack (that is, a method of attack); and a targeted asset. Using this methodology, the UK government has identified five categories of threat: physical threats to (a) people and (b) assets; information acquisition; interference with democracy; and attempts to shape the international order. It has further identified 15 vectors of attack, distributed across the categories. The presentation highlighted some of the weaknesses of the current approach, the most significant of which was a lack of prioritisation, and noted potential ‘lenses’ that might be applied to help with this. These lenses comprised prioritising those threats that were: the focus of the most hostile/capable state actors; directed at the most significant UK vulnerabilities; affected the most significant UK assets; or where the UK currently had more limited capacity to respond.

This presentation was used to frame discussion in the initial plenary session, and in two consecutive breakout sessions, which looked first at the source of threats, vectors and targets of attack, and then at UK vulnerabilities, as well as strengths and weaknesses. The meeting was concluded with a further plenary to sum up key findings. This note does not report what was said in each individual session, but gathers together participants’ insights by theme. Names and affiliations of participants are not included.

Threats to the UK

States of Concern

The participants identified ‘the big four’ – Russia, China, Iran and North Korea – as the states currently most hostile to the UK and its allies, with Russia and China the most powerful and
capable. In addition, several of these states’ allies and associates were seen as intermediate concerns – for example Belarus, Syria and Venezuela – along with current democracies such as South Africa, India, Mexico and Brazil, which had shown authoritarian tendencies or sympathy with the views and actions of Russia, China and others, as well as autocracies such as Saudi Arabia and the UAE, which seek to balance Western and non-Western interests. Turkey was noted as a particular and rising concern because of its levels of engagement with Russia and evolving authoritarianism. Several participants noted the growing levels of cooperation between Russia, Iran and, to a lesser extent, China, and expressed concern about the development of a loose group of authoritarian states coordinating their actions, which would have a potentially negative ‘multiplier effect’ on Western interests.

There was a consensus, however, that any ‘list’ of hostile states had to be treated with significant caution, and that the UK needed to avoid seeing the world as divided cleanly between a bloc of ‘friendly’ Western or pro-Western democratic states and ‘hostile’ anti-Western authoritarian states. The concept of hostile state actors needed to be viewed with nuance for a variety of reasons:

- **Theoretical versus actual hostility:** While some states such as Russia are very openly hostile to the UK and its allies – indeed have public strategies and statements to that effect – others which are allied or aligned with those powers – for example Syria, Venezuela and Cuba – show little direct hostility to the UK in practice. Moreover, some autocratic states which maintain relations with authoritarian states (Saudi Arabia and the UAE, for example), also have largely positive and non-confictual relations with Western powers, although this might change in the future.

- **Varied levels of UK focus/interest:** Despite the possibility that the UK might be affected by a hostile act, not all hostile acts are of equal intent. One breakout group noted five categories of focus, comprising: (a) acts actively targeting the UK; (b) acts directed at multiple states for the purpose of effect or damage, of which the UK was only one such state; (c) acts that use the UK as a ‘stage’, but are not intended to harm the UK per se (for example, state attacks against a diaspora resident in the UK); (d) acts which use/exploit UK-based facilities or services, such as the courts, the media or the financial system, and by doing so undermine them; and (e) acts which might be deemed a form of general state competition that occasionally cut across UK interests.

- **Damage versus intent to damage:** Some hostile states can undertake damaging acts – for example, China seeking to reshape the international economic order – which are by definition self-interested and potentially damaging to Western interests, but are not specifically intended to harm the UK or other Western states as long as these states are amenable to China’s proposed changes. Other apparently hostile states – for example North Korea – can act in a harmful way because they are in desperate straits and, as one participant put it, ‘have their backs against the wall’: North Korea’s string of crypto heists have occurred because the country needs funds, rather than because it has a specific desire to hurt the target, in this instance. At the same time, avowedly friendly states can undertake activities which can damage the UK unintentionally – such as the release of malware used in cyber attacks. Such damage can also be intentional – through economic espionage – while remaining friends and partners in most areas.
• **Varied levels of hostile capability:** Beyond China and Russia, the ranges and levels of hostile state capability vary enormously. For example, North Korea has the capability to create harm through cyber operations, but has more limited capacities to harm the UK in most other ways. One participant discussing work on Iran’s out-of-region activities noted that there was a significant gap between the ‘hype and reality’ around the scale of the threat posed.

• **Growing capabilities in friendly/neutral hands:** At the same time, some states that did not necessarily sit within the current expectation of being hostile were developing technical capabilities – primarily in cyber – that would have the capacity to do damage to the UK and its allies in the short to medium term, if used in a hostile manner. Several participants stressed growing proliferation of offensive cyber capabilities as a major cause for international concern.

Overall, the general view of the meeting was that the activities of Russia and China were of primary concern, because of their power, reach and clear intentions to promote their own interests using tools which directly and intentionally target the UK and its allies. Smaller states associated with these larger powers, such as Iran, North Korea, Venezuela, Syria and Belarus, each with varying regional ambitions, were in the next order, although it was recognised that their interest in the UK and their capabilities in general are varied, affecting it more sporadically. Next, there were the currently non-aligned states such as India, Pakistan and Saudi Arabia, pursuing goals which – while not intentionally aimed at the UK or Western countries – might cause damage to their interests. Finally, there was the group of neutral and/or friendly states whose deployment of their capabilities might have negative effects on the UK, regardless of their intentions. Although these latter two categories were not explicitly hostile states in terms of directing hostile acts at the UK, the potentially damaging effects of their behaviour needed to be recognised. Moreover, several participants noted how important it was to take a medium- and long-term view, as some currently non-aligned states with significant capabilities but low intent had the potential to move into one of the first two categories of concern over time.

**Vectors of Attack**

It was noted by several participants that various vectors of hostility, such as physical attacks on people and assets, could be used in short-term and tactical ways to cause immediate damage, while others, such as information operations, could be used in long-term and strategic ways to cause more fundamental corrosion and dislocation. Although many tools of attack would be specific – for example, the use of a weapon to attack an individual – there were some vectors which had both tactical and strategic value (if used cumulatively), such as cyber capabilities.

Accordingly, there was a strong emphasis among participants on the centrality of cyber capabilities, not only because of their versatility, but because of the capacity they gave states to either hide their own involvement or create a ‘false flag’ that made accurate attribution technically and diplomatically challenging.
Over the past 20 years, cyber operations have been mainly used for theft and espionage (for example intellectual property theft and economic espionage), and economic and social disruption, such as wiper attacks against major institutions or businesses. However, cyber-enabled information operations are also playing an increasingly salient role in broader efforts to contest the information space. Several researchers who worked on information operations noted that the greatest difficulties for those tackling the problem came from the multiplicity of small and apparently inconsequential actors, including AI-driven bots. Although none of these bad actors was individually important, at scale they could have a significant effect. Several states – not necessarily hostile to the UK – were also using social media as a means to target harassment of domestic critics and dissidents now based in the UK. These techniques are becoming increasingly advanced, using machine learning and ‘deep fakes’ to create sophisticated propaganda and misleading narratives. In some instances, cyber operations are also used as one of the elements in ‘combined operations’ against targets, along with other vectors of attack. China, for example, will mix violent actions on the ground (attacks on dissidents or protestors) with online social media doxing and disinformation campaigns, to maximise effect.

Linked to cyber, but with wider importance for a number of other vectors, participants noted the role played by proxies in the execution of attacks. Semi-autonomous organised crime groups and private sector contractors played an invaluable role in undertaking cyber attacks for Russia, China and Iran, often being allowed to undertake ‘free-range’ criminality overseas as long as certain state-set tasks were carried out. This could mean that cyber attacks conducted overseas by state-backed groups might not always be conducted on behalf of the state, or only partly so; for example, while a state-backed contractor in China might take hacked data and use it for state means alone, Russia might use it both for state purposes and also allow it to be sold on to the benefit of the criminal hackers themselves.

Beyond cyber operations, there was further evidence of state intelligence agencies using criminals, criminal groups and terrorists for intelligence collection, assaults, assassinations and other covert activities, as well as using oligarchs and businesspeople, corrupted politicians and officials, and tame journalists and academics as agents of influence. It was noted that there was an increasingly blurred line between state and non-state actors.

Some participants also noted how important diplomatic influence and economic statecraft were proving as perfectly legitimate and overt vectors for both China and Russia. China is playing an extremely active role in seeking to shape the rules of international economic bodies to suit its interests, while also exercising economic influence across Asia and Africa through the Belt and Road Initiative. Russia is making similar efforts. This effort, underpinned as it is with few demands regarding the upholding of human rights and democratic standards, has bought China and Russia influence among many states that would have previously looked to Western countries for support. As in other areas of activity, there is good evidence that China combines a number of vectors of approach to gain an overall outcome, seeking market dominance through economic espionage, placing economic controls on private sector companies, and using influence operations against the governments, legislatures and media of targeted countries to get its own way.
Key Targets

Although the leading hostile states do not advertise their major targets, several participants noted that at a strategic level, these were apparent from the negative effects now being felt by Western societies. In strategic terms, it appears that, separately, China and Russia are seeking to undermine the political, economic and social systems of the UK and its allies, as well as the international rules-based order, in order to make it easier to pursue their own interests unopposed. Their activities, sometimes coordinated but mostly not, affect multiple assets of Western societies, both tangible and intangible, corroding them over time, as one participant described, like ‘a death by a thousand cuts’.

These activities, strategic and tactical, have multiple targets, and, therefore, as some participants noted, it was helpful to ask which of those targets matter most to the citizens of the UK. This needed to be considered not based simply on what different UK government departments and agencies were already doing, or had resources or an institutional mandate to undertake, but also on a proper assessment of those elements most fundamental to the UK’s integrity. This includes a need to reconsider how ‘direct harm’ is currently defined, to better reflect the strategic harms posed by state threats, and to avoid the risk of adverse prioritisation. Of those elements discussed, four were particularly salient:

- **Uncorrupted elites and state institutions**: The corrosion of the UK state and political system from within was the greatest concern, as the integrity of the political elites, state institutions and elections was deemed fundamental to addressing all the other potential issues. It was noted that individuals linked to several hostile states already had significant leverage in the UK political system through donations, support for pressure groups and think tanks, and social networking with key decision-makers developed both organically and potentially by external direction.

- **Secure civil society and social cohesion**: Closely connected to the integrity of the state was the importance placed on preserving democratic freedoms and civil rights, balanced with a need to address what one participant termed the ‘poisoning of the well’ that comes from the spread of disinformation and conspiracy thinking on social media and in some broadcast media. Several participants noted that public discourse and social cohesion rested on shared agreement about some basic facts, even if their interpretation was open to debate. In the phrase made famous by Daniel Patrick Moynihan, ‘everyone is entitled to their own opinions, but not their own facts’. Without this, social cohesion was at risk and civil disturbance increasingly possible.

- **Economic security**: Several participants noted that the Covid-19 pandemic and the economic effects of the war in Ukraine – manipulated to an extent by Russia – had highlighted the fragility of the international economic system on which the UK, as a medium-sized trading economy, was highly dependent. Although during the pandemic the UK had managed to tackle most logistical challenges, shortages of certain goods had created some disturbance, and more severe economic disruption could have had

---

more dangerous social consequences. Well-managed supply-chain security and logistics were therefore deemed vital to ensuring access to vital commodities and goods at times of crisis.

- **Citizen safety:** Finally, participants also stressed the importance of the security of UK citizens. Several noted that maintaining the sense of safety from potential physical threats was vital to sustaining trust in UK institutions and social stability.

The importance of some of the targets/assets mentioned above were challenged by a small number of participants because of their lack of tangibility, making it difficult to calibrate the extent to which they are under threat. For example, some suggested that although there was anxiety around disinformation, evidence to show this was undermining social cohesion was hard to find and that perhaps, at present, the threat remained a matter of perception, rather than of hard data.

### Resilience and Vulnerability

Participants indicated that the UK had significant latent resilience in the face of current state threats. The UK remained a relatively prosperous economy, home to one of the world’s major financial centres in London. It still enjoyed a largely stable political and legal system, supported by broad public trust in the major institutions, including the civil service. It retained an internationally well-regarded higher education sector and significant expertise in science, technology, research and innovation, and had significant global soft power based on its historical reputation and an independent media, especially the BBC World Service. Moreover, it remained well-connected internationally, with close and enduring friendships with the world’s most powerful country, the US, other major players in the Anglophone world and Europe, and via ongoing Commonwealth ties.

Participants also noted that the UK had considerable ‘harder’ strengths, such as well-established and capable intelligence and security agencies, which could draw on strong international relationships in groups such as Five Eyes, as well as significant expertise in the field of cyber security, and well-developed protections for critical national infrastructure. There was also a good relationship in place between government departments and agencies and the private sector (for example, with energy, communications and the financial sector), allowing a ‘whole of society’ response to key threats.

Nonetheless, there was a recognition that these strengths were not now as strong as in the recent past, or as strong as the UK would need them to be to face current challenges. Trust in UK institutions had been eroded both at home and abroad, which had been compounded by spending cuts to some of those institutions (the BBC World Service was mentioned in this regard), but also more generally to services supported by the UK taxpayer. For example, one participant noted the importance of the role that good education and community engagement played in undermining the power of disinformation campaigns. With less funding, such work was more difficult to do.
In addition, participants suggested that some of the UK’s strengths were at the same time also significant vulnerabilities. The UK’s ethos as an open society – politically, economically and culturally – has made it a model to many. But this openness, which has involved limited, light-touch regulations of the political and financial systems for many years, founded on an assumption of the low risk of corruption, has now been challenged by an influx of money and influence from less scrupulous sources. Tied as the UK is to its self-image as a democratic and free society, it has therefore been ‘on the backfoot’ against those who are willing to use the UK’s openness both for their own interests and against the UK itself, tainting the system. One example provided was party funding, on which there appears to be no widespread political appetite for reform, despite the potential for its abuse; another was the penetration of the UK financial system by illicit funds, where efforts to improve transparency through the reform of Companies House and other, wider policy and legislative developments, had been half-hearted and under-resourced.

In a similar vein, several participants noted other inherent structural vulnerabilities of the UK political system. As with other liberal democracies, the electoral cycle in the UK was a problem, as it did not allow for long-term responses or planning without a bipartisan approach. The UK’s uncodified constitution was a further issue because of its operation on the basis of norms, many implicit and unstated, rather than explicit and codified. This ambiguity – while providing flexibility to those dealing with complex challenges – could also provide significant discretionary power to the executive that could be misused if placed in the hands of those susceptible to hostile influence.

Capacity to Respond

The discussion of resilience and vulnerabilities highlighted several key issues around the UK’s current capacity to respond to state threats. The basic view held by many in the political class that the UK remains open, fair and uncorrupted makes it more difficult to respond in those areas where this was proving to be less the case than previously. As several participants noted, it would be difficult for political leaders to address the issues if they, or their political associates, feared being in some ways linked to the corruption of the system. In the words of one participant, corruption risked becoming ‘an organ-attacking virus’, limiting the body politic’s capacity to fight back.

At a governmental level, there was broad agreement that the UK government was not currently well prepared to meet state threats, for a variety of reasons that ranged from a paucity of intelligence, to intellectual biases and institutional gaps:

- **Absence of a coherent intelligence picture/threat assessment**: Although none of the participants were currently in government service, there was a general perception that the overall intelligence picture about state threats and activity was lacking, or at least not well coordinated or shared across departments and agencies, and that there was still some confusion within Whitehall about what the concept of state threats meant. Because such threats might seem less immediate or threatening, and not seen as part
of a connected campaign, they risked being de-prioritised. There was a sense too that political and policy decisions were now being made without a sound foundation of intelligence and assessment. Although this was to some extent understandable – the concept of state threats remains nebulous – there was a common view that the UK had been more focused on other issues emanating from non-state-based actors (terrorism, serious and organised crime) for a long period, resulting in a lack of institutional knowledge and thinking around the challenges posed by state threats. This includes a lack of understanding of where, when and how non-state actors might work closely with state actors, in effect turning non-state threats into state threats. In the words of one participant, ‘we have been asleep at the wheel, and risk not even knowing when we have crashed’.

• **Prioritising commerce in state relations:** A further problem was the perceived bias in UK government thinking in its state relations. In the decades since the end of the Cold War, the UK had tended to use a commercial lens to look at how it handled its relationships with potentially difficult countries. The emphasis in relationships with China, Russia, and other similar countries had therefore been on supporting the prosperity of the UK, rather than on considering long-term security risks. As events of the past few years have shown, this had made the UK partially dependent on, or affected by the disruption of, technology (for example, Huawei), energy and commodities (for example, oil and gas, grain, fertiliser) from these states.

• **Siloed policy pillars:** The conduct of UK government tends to be run in distinctive pillars, with the implementation of domestic policies (such as health and education), and national security and financial oversight (sitting with the Treasury) operating separately. Responsible departments and agencies would rarely talk together in a constructive way about shared security issues. Despite its implicit interest in the issues around state threats, for example, the Treasury tended to act purely as the financial officer/accountant overseeing the distribution of funds, rather than as a policy voice.

• **Lack of governance and diffusion of departmental responsibility:** Participants felt that the lack of intra-government dialogue was compounded by the absence of any government department, agency or unit. Examples of these are the Office for Security and Counter-Terrorism at the Home Office, on the issue of counterterrorism, and the former Stabilisation Unit which brought together defence, diplomacy and development expertise in one unit physically co-located in what is now the Foreign, Commonwealth and Development Office (FCDO). These have an explicit mandate to drive cross-government policy on state threats. One participant noted that the National Security Council, which should provide the perfect forum for the coordination of state threat strategy, did not appear to have taken a strong lead on the issue. Operational responsibilities on state threats, such as they are, were also widely diffused across many public institutions, and are probably not recognised by most as part of their institutional mission; even where they were, however, some UK agencies were not proactive – no ‘mission management’ in the words of one participant – in comparison to similar US agencies, such as the US Treasury’s Office of Foreign Assets Control. Faced with a culture of producing tangible results, UK agencies would often prioritise targets – criminals or terrorists – where demonstrable quantitative outcomes were producible. Stretched resources also played
a role; some agencies that could in theory take a stronger role – for example the National Crime Agency, or multiple departments with responsibility across the state threats agenda in the FCDO – were already stretched to cover multiple priorities.

- **Public sector lacking the necessary skills and experience**: A significant proportion of participants raised the question of whether those currently working in the British civil service and other public sector agencies had the necessary skills, experience and capacity to tackle a problem as complex and long term as state threats. The UK continues to work on a generalist model, where many will move roles every two to three years, leading to an atrophying of long-term institutional knowledge. Many of these individuals will not move beyond their own departments or have experience beyond the public sector. Several participants mentioned that there was a regular exodus of the most highly skilled security professionals (for example, in cyber, intelligence, law enforcement and the military) into much higher paid private sector roles from which many would not return, although this has been mitigated somewhat in cyber by the National Cyber Security Centre’s Industry 100 secondment programme. However, it is important to again note that none of the participants were currently in government service, and it was acknowledged that the skills and experience gap may not be as stark as perceived from outside. What is likely to be as important, if not more so, is the issue of capacity, particularly whether current staffing levels across the civil service, law enforcement and intelligence agencies are sufficient in the face of the scale and complexity of the threat.

Beyond government, there were mixed views of the capacity of the private sector to play an effective part in a ‘whole of society’ response to state threats. The job of tackling many of the issues discussed in the meeting had already been partially outsourced to the private sector (for example, ensuring cyber resilience, identifying illicit financial activity, tackling disinformation on social media), but there were differing views on how well this had worked. Many recognised that good work was being done in support of government objectives; however, because commercial imperatives remained the priority over risk and security concerns, under-investment and doing ‘just enough’ to keep regulators happy was a common response to demands to be good corporate citizens. Senior businesspeople could be naive about the risks that they faced, not connecting the need to fulfil compliance and legal responsibilities – often seen as tick-box requirements – with business decisions that might expose the UK to security risks. Participants noted that the doing ‘just enough’ dynamic affected decision-making in the professions and other sectors such as higher education, science and technology, energy and logistics.

Some participants suggested that there was an additional problem where businesses had international interests and exposure to countries and regions in which hostile states were active. In these cases, there was a natural desire to calibrate and finesse risk management to levels that would satisfy home governments while not offending overseas governments (for example, UK banks operating in Hong Kong and mainland China). Such situations showed the underlying conflict of imperatives in UK policy (‘make money’ versus ‘do not work with authoritarian regimes’), which had not so far been resolved.
A final capacity issue raised was the role of international responsibilities and cooperation, particularly important given that the problem of state threats was shared across the UK’s allies and partners. The value of the UK’s enduring relationships with Anglophone, European and other democratic allies and partners, supported in many instances by bilateral and multilateral institutional structures, was recognised. Nonetheless, much as with the domestic handling of the issue in the UK, participants did not perceive a clear sense of shared international responsibility, or specific mechanisms through which to jointly tackle these issues. In cyberspace, and in financial and currency markets, among others, there was no common strategy or agreed standards of behaviour. States were largely taking their own paths on state threats, and prioritising their own concerns, potentially to the detriment of the interests of the wider democratic community. Moreover, as commented earlier, some states were continuing to exacerbate the problem by conducting damaging activities that might be deemed a state threat under other circumstances.

Responses and Countermeasures

The participants in the workshop were not tasked to look at potential responses to the state threats challenge, as this was to be the focus of the next scheduled meeting in May 2023. However, during the course of discussions, a range of suggestions were made, which are grouped into themes below:

Addressing Key Challenges

- **Weaponise transparency**: The UK’s openness was certainly perceived as a major vulnerability to hostile activity. However, the discussion emphasised that this could be a strength and also a means of response. Several participants argued that the UK needed to go further along the road of radical transparency in the economic and financial realm, understanding beneficial ownership of businesses, property and other assets, while translating the same approach to other areas, such as party funding, think tanks and political consultancies, to make the UK less attractive to those who have sought to misuse its freedoms in the past. The UK should become a jurisdiction where it is easy to ‘follow the money’.

- **Strengthen the system**: One of the most persistent concerns expressed throughout was the risk of the UK political system and state institutions being corrupted from within. Proposals to improve the transparency of political funding, noted above, were one response to this, while others included the need to strengthen explicit checks and balances around the use and abuse of executive powers, clear standards (see the Nolan Principles), independent oversight of ministerial behaviour ethics, and appropriate and consistent vetting for ministers.

Strategies and Structures

- **Map assets, vulnerabilities and threats**: The UK government should prioritise those key assets – tangible and intangible – that it matters most to protect, map major vulnerabilities, and develop a full-spectrum intelligence picture of which state actors
are threatening it, as well as both the tactical and strategic methods being used. The UK government should also take a longer-term view of state intentions and capabilities which could be deployed in a hostile way in the future, and ensure threat assessments remain up to date. A fusion approach would be vital as part of this, to ensure that connections currently being missed are being drawn across the whole of the UK’s intelligence community.

- **Rejuvenate strategy and governance**: The UK government needs to develop a unified cross-government view and strategy in response to the state threats challenge that enjoys the same level of energy and ministerial support as Contest. To make this feasible, the government needs to either refresh existing machinery (such as the National Security Council), or create new mechanisms, through which a strategic policy response can be developed and managed. Any response needs to include the role of international and domestic private sector cooperation from the start, rather than as a later ‘add-on’ or ‘nice to have’.

- **Embed the ‘security perspective’**: While few participants wished to go as far as the wholesale securitising of UK policy, most agreed that the security perspective needed greater weight in future decision-making, especially in relation to the current prioritisation of commerce over security. This meant the need for longer-term perspectives about working with overseas companies in key infrastructure projects, or the extent to which companies from potentially hostile countries would be allowed to penetrate important British industries or markets. The UK also needs to ‘pre-position’ and play a longer game within international organisations, working with coalitions of countries to ensure the attempt by China and others to reshape the international economic environment against Western interests was less impactful.

- **Improve agency resources and capabilities**: Participants noted that the UK was facing tighter public finances, but at the same time, it was suggested that an infusion of new funds and resources would be required, much as had happened to the intelligence agencies after the 9/11 attacks and the London bombings in July 2005. It made no sense to repurpose existing capabilities for the ‘flavour of the day’ alone, thus leaving other ongoing areas of concern, such as counterterrorism, without coverage. Several participants noted that the National Crime Agency was not resourced to undertake significant work on illicit financial and organised crime activities with a national security dimension, and its prioritised focus on UK direct harms may prove challenging, at least in the short term, for the transition needed for a more strategic national security-focused approach. Identifying the unique contributions of different agencies and departments and the sorts of expertise, capabilities and capacity needed across departments should be prioritised. Consideration also needed to be given to how to better retain staff with relevant skills and experience, as well as looking at how investments in research related to state threats may also better contribute to building capabilities.

- **Promote realistic public–private partnerships**: Participants mentioned how some governments, such as those of Taiwan and Israel, would expect businesses to put national security imperatives above commercial drives because of the perceived existential threats facing the country. This was not seen as a credible possibility in the UK, going against the current mindset and ethos of both government and business. This
said, several suggested that more could be done to mature partnerships with those parts of the private sector affected by state threats (for example social media), potentially through regulatory or commercial incentivisation, stronger state direction, and greater operational cooperation to identify and disrupt a wider range of bad actors. A number of participants further suggested it would be important to also involve elements within civil society that undertook research and investigations into issues such as disinformation and corruption.

The International Dimension

- **Promote proactive international action**: As noted above, participants believed that the UK should take a more proactive international position, rather than simply reacting or acquiescing to the activity of China, Russia and others. These powers were seeking to make the world more amenable to their interests, and Western powers could no longer afford to behave in a ‘business as usual’ manner. A ‘forward defence’ approach would require the UK to invest more in its diplomatic capabilities, look again at overseas development support and aid, and revive key elements of soft power, such as the BBC World Service, which were currently under-resourced. The UK should also be seeking to push back by building on existing relationships with countries within hostile states’ perceived ‘spheres of influence’, such as those of Central Asia, while also using its influence more consistently in its own Overseas Territories and Crown Dependencies, several of which have been used by hostile state actors for illicit financial purposes.

- **Promote realistic international partnerships**: There was broad agreement that the UK had to work closely with international partners on this issue, requiring the development of a shared view and approach. However, it was recognised that divergent interests and priorities would create some frictions – as seen even with the response to the full-scale Russian invasion of Ukraine – and that maintaining a broad front would likely require taking a narrower, rather than broader, view of state threats. In this regard, the UK would need to recognise that what might be termed ‘damaging behaviour’ by friendly states would be more difficult to address, although dialogue about state threats might open some options for agreed standards of international behaviour in key areas where capability matters as much as intent, such as cyber proliferation.

- **In conclusion**, several participants emphasised the need to take a carefully calibrated approach to handling state threats, to minimise negative unintended consequences. While the UK needed to recognise the security aspects of more aspects of society, it had to avoid over-securitising its approach to the extent that it fundamentally altered the society’s open nature. It also needed to avoid taking so aggressive an approach that it drove away foreign investment or talent. Moreover, it needed to avoid a stridency that would prove counterproductive internationally, pushing non-aligned countries further towards already-hostile states. A narrative based on ‘Western values’, or ‘the West versus the rest’, would play into the hands of Russia and China. Any international rhetorical approach therefore needed to stress universal values – and shared interests – to refute any alternative claims.