Briefing Note 37
July 2025

SOC ACE Serious Organised Crime & Anti-Corruption Evidence Research Programme

Old Wine, New Bottles? The Challenge of State Threats[1]

Matthew R. Redhead[2]

Summary

Over the past decade, Western countries have faced a rising tide of hostile actions perpetrated by state actors and their partners; many sit in the so-called grey zone between peace and war and use hybrid methods of attack.[3] This body of activities has become known in Western policy circles by a variety of terms, such as "threats from state actors", "hostile activity by states", or "state threats" – the term currently used by the UK government.[4] Much of the current discourse around state threats has been poorly and loosely defined, however, and has failed to ask basic questions such as why state threats are so important now.

This briefing note summarises research that addresses these and other concerns,[5] looking to provide firmer definitional boundaries and explore the scale, scope and character of modern state threats within them. Certainly, there is much that is familiar about state threats; many of the actions that fall under its broad umbrella are well-known covert and clandestine acts such as espionage, repression, sabotage, subversion and malign influence, and are closely associated with long-term adversaries of the West, such as Russia, China, Iran and North Korea.[6] However, the research notes that besides the apparent explosion in the volume and range of hostile activity, much is new in their execution and operationalisation. Contemporary state threats combine traditional intelligence tradecraft with new technologies, exploit vulnerabilities that never existed before in societies and economies, and are increasingly outsourced to non-state actors with niche skills, physical access and higher risk tolerances than state agencies. State threats are also not just the preserve of familiar adversary states, with "middle powers" using them as tools of statecraft.[7]

The research finds that state threats' relative cheapness and deniability allow states to attempt to undermine, coerce and influence their opponents, with limited risk of starting a major war, making them attractive tools for politically

---

1 For the full research paper, see: Redhead, M. (2025). *Old Wine, New Bottles? The Challenge of State Threats.* SOC ACE Research Paper No. 32. Birmingham, UK: University of Birmingham. https://www.socace-research.org.uk/publications/soc-ace-rp32-state-threats

2 Matthew Redhead, Senior Associate Fellow, Royal United Services Institute, is a former UK government employee and senior financial crime professional. All correspondence to matthewr@rusi.org

3 For an overview of the conceptualisation and reality of grey zone conflict and hybrid war, see: Kilcullen, D. (2020). *The dragons and the snakes: How the rest learned to fight the West*. Hurst & Company.

4 Algemene Inlichtingen- en Veiligheidsdienst (AIVD) Militaire Inlichtingen- en Veiligheidsdienst (MIVD) & Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2022, November). *Threat assessment state sponsored actors 2 (TASA).* https://english.aivd.nl/publications/publications/2023/02/13/threat-assessment-state-sponsored-actors-2-tasa; Home Office. (2021, 13 May). *Legislation to counter state threats (hostile state activity)* [Government consultation]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986013/Consultation_Document_-_Legislation_to_Counter_State_Threats.pdf; Public Safety Canada. (2022, 25 April). *Parliamentary Committee notes: Countering hostile activities by state actors*. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20220930/06-en.aspx

5 This Briefing Note is the first in a series providing short summaries of key thematic and geographic aspects of the research, all of which will be available on the project website: Understanding State Threats. https://www.socace-research.org.uk/projects/socace-rusi-understanding-state-threats

6 Listed in order of perceived current relative threat level to the UK.

7 Middle powers are loosely defined as states that sit below global powers such as the US, China and Russia in terms of political, economic or military power and influence. They comprise both developed and developing economies, but the majority of those that are developed are tied into Western economic and security structures. See: Elliott, D. (2024, 26 January). Middle powers: what are they and why do they matter? *World Economic Forum*. https://www.weforum.org/stories/2024/01/middle-powers-multilateralism-international-relations/

assertive states in a time of rapid geopolitical change. Although the impact of hostile actions on Western states has so far been mixed, they have the potential to become more damaging over time as societal resilience wears down, new technologies emerge, hostile actors' risk tolerances increase and more states participate.

Background

In 2024, the UK faced a wave of state-linked hostile actions within its borders and against its interests. These hostile actions included, but were not limited to, extensive Chinese cyber espionage against UK political, military and commercial targets; Russian espionage, cyber attacks and physical sabotage against supplies to Ukraine; and Iranian attempts to harass and assassinate dissident journalists living in the UK.[8]

According to officials, state-linked hostile activity in the UK has risen dramatically over the past decade. In March 2023, the assistant commissioner of the Metropolitan Police, Matt Jukes, stated that his force's casework on foreign interference and espionage had increased fourfold since March 2018, with the attempted poisoning of former Russian intelligence officer Sergei Skripal in Salisbury.[9] This experience has been mirrored across liberal democracies in Europe, North America and the Asia-Pacific region.[10] Consequently, many of these countries' governments have begun to develop specific policies to respond to the threat of state-backed hostile activity.[11] The problem these policies seek to tackle has been described in various ways, with the UK choosing the term "state threats".[12]

In response to the growing importance of state threats and a limited body of research on the issue, the Serious Organised Crime & Anti-Corruption Evidence research programme worked with the Royal United Services Institute to set up the inter-disciplinary State Threats Taskforce (STT) in 2023. The STT convened two workshops comprising former practitioners and experts from Europe and Five Eyes countries,[13] which sought to scope the threat landscape faced by the UK and its allies, and current and potential policy responses.

While helping to sketch the outlines of the challenge, however, the workshops revealed uncertainty – even among those deeply immersed in relevant fields – about fundamental questions, such as the meaning of the term state threats.[14] To address these issues, this research was developed to:

1. Clarify the meaning and coherence of the term state threats.
2. Understand why state threats have emerged as an issue now.
3. Map out the scope and nature of current state threats.
4. Assess the effectiveness of hostile activity as a tool of state policy.
5. Consider the potential development in the state threats landscape in the short-to-medium term (two to five years, following definitions of duration common in government and business).

Evidence was collected through a desk review of research literature, publicly available official documents, and credible media reports published in English over the previous decade, supplemented by 50 semi-structured interviews with academic experts, researchers, journalists, current and former government officials, and practitioners the Asia-Pacific region, Europe and North America. Interviewees were selected based on their knowledge and expertise on state threats or related areas, specific domains such as cyber or disinformation, and/or specific countries and regions, and provided new insights, further case studies and examples, and validation of emerging findings as the research progressed.

---

[8] Dowden, O. (2024, 25 March). Cyber security and UK democracy. *Hansard*. UK Parliament. https://hansard.parliament.uk/commons/2024-03-25/debates/096EB6E9-21A1-40A5-A7F4-247C52AFC070/Cyber-SecurityAndUKDemocracy; Mackintosh, T. (2024, 3 April). *Pouria Zeraati: Three accused of TV presenter attack have left UK*. BBC News. https://www.bbc.co.uk/news/uk-england-london-68717210; Sandford, D. (2024, 26 April). *Two British men charged with helping Russian intelligence*. BBC News. https://www.bbc.co.uk/news/uk-68899130

[9] Casciani, D. (2023, 16 February). *Hostile-state threat probes grown fourfold – police.* BBC News. https://www.bbc.co.uk/news/uk-64668063

[10] Various examples are provided in: Braw, E. (2022). *The defender's dilemma: Identifying and deterring gray-zone aggression*. AEI Press; Cormac, R. (2022). *How to stage a coup and ten other lessons from the world of secret statecraft*; Galeotti, M. (2022). *The weaponisation of everything: A field guide to the new way of war*. Yale University Press.

[11] AIVD et al. (2022); Australian Security Intelligence Organisation (ASIO). (n.d.). *Recognising hostile intelligence activity*. https://nitro.asio.gov.au/recognising-hostile-intelligence-activity/; Home Office (2021); Public Safety Canada (2022).

[12] Royal United Services Institute (RUSI). (n.d.). *RUSI State Threats Taskforce (STT)*. https://rusi.org/explore-our-research/projects/rusi-state-threats-taskforce-stt

[13] Five Eyes is the term used for an intelligence-sharing arrangement between Australia, Canada, New Zealand, the UK and the US.

[14] Royal United Services Institute (RUSI). (2023a, March). *State Threats Taskforce: 'Assessing the threats'* [Conference report]. https://static.rusi.org/393-CR-SST-Meeting-One-State-Threats-web-final-updated.pdf; Royal United Services Institute (RUSI). (2023b, June). *State Threats Taskforce: 'Assessing the responses'* [Conference report]. https://www.rusi.org/explore-our-research/publications/conference-reports/rusi-state-threats-taskforce-assessing-responses

Key findings

Defining state threats

Western governments and international organisations such as the European Union (EU) and the North Atlantic Treaty Organization (NATO) use various terms for hostile activities by states; unsurprisingly, these meanings vary.[15] While terms such as "state threats" or "hostile activity by states" sound identical, their scope can differ; for example, the UK government includes overtly hostile acts, whereas several other governments do not. Moreover, all current government definitions have ambiguities, especially around the importance of hostile intent and levels of state responsibility. Some harmful acts are not necessarily hostile as such – failing to meet climate change commitments, for example – and harmful acts undertaken by non-state actors with state links are not always undertaken at that state's behest.

To clarify these issues, the research sets out a new "working model" definition for state threats that combines the most common elements of existing definitions and seeks to draw pragmatic boundaries where uncertainties exist. Four criteria are identified:

1. **Severity**: State threats are hostile acts that fall short of the internationally defined nature of war and/or distort and subvert peacetime international rules and norms.
2. **Source**: State threats are initiated or encouraged by a state actor and executed by a state or non-state actor for the initiating state's purposes.
3. **Character**: State threats are underhand and, by nature, covert, deceptive, corrupt, illegal, coercive and threatening. They may also abuse international rules and norms to achieve hostile ends.
4. **Intention and effect**: State threats cause intentional and politically motivated damage to the interests and assets of another state (or states).

This definition makes clear that state threats must include an intention to cause harm. Certainly, negligent or anti-social behaviour by states, or even positive behaviour which creates dependencies, can be "weaponised" for nefarious purposes at some future point. These types of behaviour should thus be seen as potential vulnerabilities that might become future targets for hostile action. But they should not be treated as immediate threats unless there is evidence of malign intent. Moreover, while all harmful acts of non-state actors cannot be ascribed to states with which they have links, if there is evidence of interaction between a non-state actor and a state, combined with an alignment in hostile behaviours – whether in method, target choice or timing – there are reasonable grounds for seeing non-state actions as state threats.

The state threats "moment"

The fundamental reason for state threats' increasing prominence is mounting hard evidence. Where quantitative data about state-linked hostile actions are available – in the fields of cyber espionage and offensive operations, or online disinformation, for example – the consistent indications are that state involvement is on the rise, with states such as Russia, China, Iran and North Korea playing major roles.[16] These quantitative data are reinforced by numerous qualitative assessments from officials, and intelligence and law enforcement officers in Western countries.[17] However, this is not the only reason why governments are paying attention now. The geopolitical context of the past decade, with events such as Russia's seizure of Crimea in March 2014 and its full-scale invasion of Ukraine in February 2022, have forced Western governments to look at these states' hostile activities in a new light. What were previously treated as bearable frictions to be downplayed in the interests of maintaining good political and economic relations have increasingly been seen as indications of deep-seated aggressive intentions.[18] Other shifts in the security environment over the past decade have also played a role. While terrorist attacks have continued, government efforts to degrade terrorists' operational capabilities have helped reduce their impact in comparison to the

---

[15] AIVD et al. (2022); ASIO (n.d.); Home Office (2021); Hybrid CoE. (n.d.). *Hybrid threats as a concept.* https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/; Public Safety Canada (2022).

[16] See, for example: Council on Foreign Relations (CFR). (n.d.). *Cyber operations tracker* [Data set]. https://www.cfr.org/cyber-operations/; Center for Strategic and International Studies (CSIS). (n.d.). *Survey of Chinese espionage in the United States since 2000* [Data set]. https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000; Maness, R.C., Valeriano, B., Hedgecock, K., Macias, J.M., & Jensen, B. (2023). Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID): Cyber conflict from 2000-2020, *The Cyber Defense Review, 8*(2), 78. https://cyberdefensereview.army.mil/Portals/6/Documents/2023_Summer/Maness_Macias%20et%20al%20CDR%20V8N2%20Summer%202023.pdf?ver=iJDHRpDvaq-hW4Zde6EwUg%3d%3d

[17] See, for example, McCallum, K. (2022, 16 November). *Annual threat update* [Transcript]. MI5. https://www.mi5.gov.uk/news/director-general-ken-mccallum-gives-annual-threat-update; Rathbone, J.P., & Reed, J. (2024, 14 May). China poses 'genuine and increasing cyber risk' to UK, warns GCHQ head. *The Financial Times*. https://www.ft.com/content/22249735-29ed-4902-8a43-482943ae3323; Wray, C. (2020). *The threat posed by the Chinese government and the Chinese Communist Party to the economic and national security of the United States* [Transcript]. Federal Bureau of Investigation. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states

[18] David, M., & D., L. (2024). Russia's war on Ukraine: unbottled emotions and the conditioning of the EU's Russia policy. *Journal of European Integration 46*(5), 661-684. https://doi.org/10.1080/07036337.2024.2363613; Lough, J. (2021). *Germany's Russia problem: The struggle for balance in Europe* (pp. 155-192). Manchester University Press.

attacks of the early years of the 21st century.[19] The relative decline in the scale and lethality of such attacks has helped open "policy space" to address the challenge posed by state-linked hostile acts.

Mapping state threats

The research provides a survey of current threats in practice, outlining key areas of hostile activity, examining the methods or vectors of hostile action, and highlighting common targets and purposes behind attacks. Some types of hostile activity are overt. China has employed public diplomatic threats, commonly referred to as "wolf warrior diplomacy",[20] which imply dire consequences for states that do not comply. Similarly, Russia has made verbal threats against its European neighbours, supported by blatant displays of military force near international boundaries, termed "heavy metal diplomacy" by Russia expert Mark Galeotti.[21]

Covert and clandestine measures

Contemporary state threats are more frequently clandestine or covert, however. The research identifies seven key areas of covert or semi-covert hostile activity:

1. **Espionage** against state, military and political targets, as well as commercial and knowledge-focused espionage.
2. **Intimidation** of dissidents and critics, including harassment, surveillance and "lawfare",22 through to kidnapping and assassination.
3. **Sabotage**, including offensive cyber operations and the "systemic overload" of social systems through the weaponisation of criminal activities such as illegal migration.
4. **Subversion** of the information environment to shape the views, actions and decision-making of audiences within a targeted state or states.
5. **Malign influence** over elite figures and groups with the power and position to guide the public policy of a targeted state.
6. **Sponsorship of groups** seeking to destabilise the existing political order of a targeted state.
7. **Orchestration of regime/government change** through support for coups d'état or direct interference in electoral processes.

Origins and execution

The research examines the mechanics behind the initiation and execution of these hostile activities, to the extent possible given their largely secretive nature. Narratives shaped by Western news media frequently portray authoritarian leaders as closely guiding or directing the activities of their bureaucracies.[23] However, the research reveals that state threats can arise from a variety of sources, including "business as usual" official processes, the self-direction of intelligence agencies, and freelance efforts by senior officials or influential private figures, as well as direct requests from state leaders themselves. To further complicate this picture, the research also finds that the operatives employed to carry out hostile acts vary; while intelligence officers remain central to state threat operations, other state officials, party officials and non-state actors are increasingly involved. These include mostly legitimate actors in the private sector, civil society and diaspora communities, alongside the more clandestine realms of private military companies, organised crime, political extremism and terrorism.

Patterns of activity

Although the research does not conduct a quantitative analysis of state threat cases, it does highlight evident trends and patterns in the qualitative evidence from recent years:

- There have been "booms" in commercially focused espionage, cyber operations and online disinformation[24] – activities in which technology and "whole-of-society" approaches can enable states to collect high volumes of information and penetrate sensitive systems at speed.[25]
- State actors have increasingly incorporated cyber tools into established forms of tradecraft, such as espionage, intimidation, sabotage and malign

---

[19] Reimer, S., & Redhead, M. (2021, May). *A new normal: Countering the financing of self-activating terrorism in Europe* [Occasional paper] (pp. 1, 7). Royal United Services Institute. https://static.rusi.org/265_op_lone_actor_0.pdf

[20] Martin, P. (2021). *China's civilian army: The making of wolf warrior diplomacy.* Oxford University Press.

[21] Galeotti, M. (2019). *Russian political war: Moving beyond the hybrid* (pp. 71-73). Routledge.

[22] Lawfare was coined in a military context by former US air force general Charles Dunlap to mean 'the use of law as a weapon of war'; Dunlap, Jr, C.J. (2001, 29 November). *Law and military interventions: Preserving humanitarian values in 21st century conflicts* [Conference paper]. Humanitarian Challenges in Military Intervention Conference, Carr Center for Human Rights Policy Kennedy School of Government, Harvard University Washington, DC. https://people.duke.edu/~pfeaver/dunlap.pdf].

[23] Chotiner, I. (2020, 23 January). How Putin controls Russia. *The New Yorker*. https://www.newyorker.com/news/q-and-a/how-putin-controls-russia

[24] Bradshaw, S., Bailey H., & Howard, P.N. (2021). *Industrialized disinformation: 2020 Global Inventory of Organised Social Media Manipulation* [Working paper 2021.1]. Project on Computational Propaganda, Programme on Democracy & Technology, Oxford Internet Institute. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/cybertroop-report20-draft9.pdf; CFR (n.d.); CSIS (n.d.); Maness et al. (2023).

[25] For discussions of Chinese and Russian varied "whole of society" approaches, see: Eftiamides, N. (2020). *Chinese espionage: Operations and tactics*. Vitruvian Press; Galeotti, M. (2019, pp. 93-100).

influence, where technology complements and enhances human activity rather than replacing it.[26]

- Different states have evolved varied national styles of hostile activity, such as Russia's high-risk and brazen approach, Iran's reliance on non-state partners, North Korea's ambitious cybercrime spree and China's more carefully calibrated approach.[27] Each style is shaped by that state's resources, ambitions, cultures and histories.

The research also confirms the widespread Western perception that contemporary state threats are largely emerging from four authoritarian regimes – China, Russia, Iran and North Korea – and that liberal democracies are among the major targets. However, it also indicates that hostile acts are not solely the province of authoritarian states and Western countries are not the only victims. In fact, hostile acts between states occur in a variety of contexts, especially among emerging middle powers. Authoritarian and autocratic states have targeted local rivals in conflict zones such as the Middle East,[28] and democratic states such as India have allegedly used hostile acts against state rivals and dissidents both within their own regions and sometimes within the borders of Western states.[29]

Motives

What is shaping these patterns of behaviour? The research suggests that each of the four most hostile states in question has its own distinctive culture, history and ambitions but is also subject to broader trends at work. At macro-level, what the research sees as "geopolitical climate change" is fundamental. Leading non-Western powers such as China and Russia have long preferred a world order shaped by great powers, spheres of influence and state sovereignty, instead of a Western vision of a rules-based international order dominated by the US.[30] Now, with the shift of economic and political power away from the US and its allies, China and major developing economies not only have a desire to see the world work in support of their interests, but they also have the strength to make it happen – the kind of historical turning point that has often resulted in open war in the past.[31] However, although China and other states enjoy growing economic and military strength relative to the West, open conflict could entail substantial and even existential risks. Consequently, hostile acts that fall short of war offer alternative ways to signal resistance to Western states and undermine Western interests, while avoiding the threat of a substantial response.

What motivates the wider use of hostile actions beyond the four main perpetrators? Many of the states in question are located close to conflict zones or in high-risk regions, and have used covert and clandestine means against their exiled opponents and local enemies for many years. However, even among the middle powers, there are indications that the use of state threats is on the rise and that this too is probably one of the effects of geopolitical climate change. With the US and its allies both less willing and less able to play the role of global law enforcer, smaller states are taking matters into their own hands, but without risking open conflict: in the words of political scientist Ivan Krastev, they 'are determined to be at the table, and not on the menu'.[32] There is also a possibility that states are emulating patterns of behaviour they see other states using with relatively little consequence. As international relations scholar Shogo Suzuki has suggested, the development of "delinquent gangs" among states can, over time, lead to a wider contagion of behaviours between states that were previously seen

---

[26] For examples of the interactive roles of technology and human assets in clandestine and covert activities, see: Eftiamides, N. (2020); Riehle, K. (2022). *Russian intelligence: A case-based study of Russian services and missions past and present* (pp.235-260). National Intelligence University, United States Government.

[27] For national examples, see: Giles, K. (2023). *Russia's war on everybody – And what it means for you*. Bloomsbury Publishing; Greitens, S.C. (2014). *Illicit: North Korea's evolving operations to earn hard currency*. Committee for Human Rights in North Korea. https://www.hrnk.org/documentations/illicit-north-koreas-evolving-operations-to-earn-hard-currency/; Jones, S.G. (2023). Soleimani, Gerasimov, and strategies of irregular warfare. In H. Brands (Ed.), *The new makers of modern strategy: From the ancient world to the digital age* (pp. 996-1021). Princeton University Press; Joske, A. (2022). *Spies and lies: How China's greatest covert operations fooled the world*. Hardie Grant Books; White, G. (2022). *The Lazarus heist: From Hollywood to high finance: Inside North Korea's global cyber war*. Penguin.

[28] A leading example in the region is the UAE, on which, see: Freeman, B. (2021, 27 July). *Hold the UAE accountable for meddling in US politics.* Defense One. https://www.defenseone.com/ideas/2021/07/hold-uae-accountable-meddling-us-politics/184052/; Krieg, A. (2023). *Subversion: The strategic weaponization of narratives* (pp. 146-174). Georgetown University Press.

[29] Cecco, L. (2024, 5 April). India and Pakistan tried to meddle in Canada elections, spy agency says. *The Guardian*. https://www.theguardian.com/world/2024/apr/05/india-pakistan-interfere-canada-elections; Ellis-Peterson, H., Hassan, A., & Baloch, S.M. (2024, 4 April). Indian government ordered killings in Pakistan, intelligence officials claim. *The Guardian*. https://www.theguardian.com/world/2024/apr/04/indian-government-assassination-allegations-pakistan-intelligence-officials#:~:text=The%20majority%20of%20those%20allegedly,which%20have%20killed%20hundreds%20of; Rathbone, J.P., & Reed, J. (2023, 20 September). India's foreign spy agency drawn out of the shadows by Canadian allegations. *The Financial Times*. https://www.ft.com/content/764a8989-ceac-4fff-85db-bc130f913f82

[30] For discussions of Chinese perspectives on the world order, see: Economy, E.C. (2023). *The world according to China* (pp. 1-28, passim). Polity Press; and Tsang, S., & Cheung, O. (2024). *The political thought of Xi Jinping* (pp. 168-193). Oxford University Press. For Russia, see: Contessi, N. (2016). Prospects for the accommodation of a resurgent Russia. In Paul, T.V. (Ed.), *Accommodating rising powers: Past, present, and future* (pp. 268-289). Cambridge University Press; Giles, K. (2019). *Moscow rules: What drives Russia to confront the West* (pp. xv-68). Royal Institute of International Affairs; and Lewis, D.G. (2020). *Russia's new authoritarianism: Putin and the politics of order* (pp. 161-192). Edinburgh University Press.

[31] Paul, T.V. (2016). The accommodation of rising powers in world politics. In T.V. Paul (Ed.), *Accommodating rising powers: Past, present, and future* (pp. 3-32). Cambridge University Press.

[32] Krastev, I. (2022, 18 November). Opinion: Middle powers are reshaping geopolitics. *The Financial Times*. https://www.ft.com/content/0129492d-ac7f-4807-8050-2760a09e9ccc

as unacceptable by the international community.[33]

Novelty and effectiveness of state threats

Those with sceptical views of the potential impact of clandestine and covert action use various arguments: that such activities are not new and have not had an impact in the past; that they are inherently difficult to execute successfully and therefore have limited value as policy tools; and that their results are never certain and, indeed, can be counterproductive.[34]

To be sure, state-backed hostile activities are not a complete novelty, and have a long and continuous global history, even during relatively peaceful periods. Nonetheless, the research finds it hard to understate the sheer volume of hostile activity currently being registered by senior Western intelligence officials, who have used language that frames the current wave of hostile acts in distinctly "epic" and "epoch-making" terms.[35]

Besides the explosion in volume, moreover, there is much that *is* new in the way contemporary state threats are executed. Cyber tools play an increasingly important role in well-known activities such as espionage, harassment, sabotage and disinformation. Importantly, however, cyber has not so much replaced traditional human intelligence tradecraft, but has been combined with it, creating a form of technologically augmented clandestine and covert action, providing opportunities for a greater volume, velocity and range of hostile acts.

Also new is the comprehensiveness of the approaches being used by China and Russia; their whole-of-society strategies have expanded the range of channels they use to conduct their activities, and they have strayed far from the classic state agency foci of official, military and political targets into the commercial, scientific and even societal realms as well. As Russia expert Keir Giles says of the Kremlin's online campaign against dissent and overseas criticism, 'it is a profound mistake for anybody to assume that they are too unimportant to be a target'.[36]

The research also offers a cautious perspective on the question of effectiveness. To be sure, the picture is mixed. As intelligence historian Rory Cormac points out, few covert acts have unambiguously positive or long-term results for the perpetrators. Critics have not been cowed, Western economies have not been crippled and most Western governments have largely remained true to pre-existing policies.[37] In fact, many of these hostile acts have also come at significant reputational cost to the perpetrators, as well as leading to policy countermeasures such as sanctions, prosecutions and the expulsion of intelligence operatives, which have the perverse effect of reducing the perpetrators' long-term capabilities and access to their targets.[38]

Nonetheless, this optimistic perspective might prove misguided, as the research notes several examples of hostile state action that cannot be seen as anything other than successes. China's massive campaign of commercial espionage has certainly reaped an enormous economic dividend. In the words of General Keith Alexander, former head of US Cyber Command, it has probably been 'the single greatest transfer of wealth in history'.[39] North Korea's cybercrime spree of recent years has also probably netted it many billions in US dollars' worth of cryptocurrency, propping up the regime of Kim Jong Un and allowing it to continue its development of weapons of mass destruction.[40] In other cases, hostile efforts might have played a contributory role in enabling the perpetrator's desired outcome; some, though not all, see Russian interference in the US 2016 presidential election as a potential

---

[33] Suzuki, S. (2017). 'Delinquent gangs' in the international system hierarchy. In A. Zarakol (Ed.), *Hierarchies in world politics* (pp. 219-240). Cambridge University Press.

[34] For discussions of the novelty and effectiveness of various covert and clandestine activities, see: Daugherty, W.J. (2010). Covert action: Strengths and weaknesses. In L.K. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 608-625). Oxford University Press; Freedman, L. (2017). *The future of war: A history* (pp. 222-238). Penguin Books; Maschmeyer, L. (2021). The subversive trilemma: Why cyber operations fall short of expectations. *International Security 46*(2), 51-90. http://dx.doi.org/10.1162/isec_a_00418; Rid, T. (2017). *Cyber war will not take place* (pp. vii-x, passim). Oxford University Press; Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare* (pp. 421-435). Profile Books; and Smeets, M. (2022). *No shortcuts: Why states struggle to develop a military cyber-force* (pp. 1-12, passim). Hurst & Company.

[35] McCallum, K. (2022, 16 November); Rathbone, J.P. (2024, 14 May).

[36] Giles, K. (2023, p. 155).

[37] Cormac, R. (2022). *How to stage a coup and ten other lessons from the world of secret statecraft* (pp. 252-274). Atlantic Books.

[38] Riehle, K. (2022, p. 262); Riehle, K.P. (2024). Ignorance, indifference, or incompetence: Why are Russian covert actions so easily unmasked? *Intelligence and National Security 39*(5), 864-878. https://doi.org/10.1080/02684527.2023.2300165

[39] Alexander, K.B. (2015, 3 November). *Prepared statement of Gen (Ret) Keith B. Alexander on the future of warfare before the Senate Armed Services Committee* (p. 3). US Senate Committee on Armed Services. https://www.armed-services.senate.gov/imo/media/doc/Alexander_11-03-15.pdf

[40] Chainalysis (2024, February). *The 2024 crypto crime report* (p. 43). https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf; Fischerkeller, M., & Harknett, R. (2023). Cyber persistence, intelligence contests, and strategic competition. In R. Chesney & M. Smeets (Eds.), *Deter, disrupt, or deceive: Assessing cyber conflict as an intelligence contest* (pp. 109-133). Georgetown University Press; Nakamura, R., & Kobara, J. (2023). *'North Korea gets half its foreign currency from cyber theft': US official.* Nikkei Asia. https://asia.nikkei.com/Spotlight/N-Korea-at-crossroads/North-Korea-gets-half-its-foreign-currency-from-cyber-theft-U.S.-official#:~:text=North%20Korea%20gets%20half%20its%20foreign%20currency%20from%20cyber%20theft%3A%20U.S.%20official,-Washington%20seeks%20clampdown&text=SINGAPORE%20%2D%2D%20The%20U.S.%20estimates,senior%20American%20official%20told%20Nikkei.

example.[41] Moreover, immediate or consistent "results," as often demanded by Western governments, may not necessarily be the aim of many of these actions. States employing hostile actions might have varying metrics of success; they may be content with achieving only an occasional "lucky hit" or expect that actions will have a measurable impact on their targets' resilience over the medium-to-long term.[42] It is also conceivable, as political scientists Austin Carson and Karen Yarhi-Milo argue, that states engaging in covert actions view those actions as means to "signal" credibility, strength and intent to other governments, without the accompanying risks associated with military action.[43]

State threat futures

Despite the challenges Russia has faced in Ukraine, Iran's recent setbacks in the Middle East and North Korea's noticeable economic difficulties, all three continue to possess the apparent will, intent and sufficient means to pursue their current range of hostile activities. In some cases – Russia, for example – there also appears to be a growing willingness to take greater risks, escalating levels of violence and the potential threat to life.[44] Most importantly, China boasts vast capabilities and, particularly in the realm of offensive cyber operations, has been demonstrating a heightened level of aggressiveness and readiness to pre-position assets for acts of sabotage against Western infrastructure, presumably in preparation for a potential future crisis in the South or East China Seas.[45]

Given the relative openness of Western economies, societies and systems, all four revisionist states[46] have good access to potential targets and, where they do not, can work with a range of deniable partners and proxies that do – especially in the criminal fraternity.[47].

As new technologies such as varieties of artificial intelligence (AI) and quantum computing develop,[48] opportunities for these states to enhance and extend their capabilities will also grow, although policymakers should be cautious about magnifying the effect they will have; advanced technologies can be hard to deploy and have defensive as well as offensive possibilities.[49]

In addition to the four main current perpetrators of state threats, the research predicts their increasing use by middle powers, particularly in the Global South. As the US and other Western powers withdraw from direct involvement in regional conflicts in areas such as the Sahel, Southern Africa, the Middle East and South-East Asia, local powers are likely to become more inclined to employ tools that can assist them in damaging, deterring or influencing rivals without triggering conflict. Middle powers' use of state threats is most likely to occur in the deployment of cyber tools for transnational repression, espionage, offensive cyber operations and online information operations.[50] At the same time, the experience of the past decade suggests that these states might become more ambitious, daring, physical and kinetic over time, and, like the current four states of concern, increasingly turn towards non-state partners and proxies to supplement their capabilities. There is also a risk that some liberal democracies will be increasingly tempted to expand their own use of aggressive activities below the threshold of armed conflict in response to the changing international environment, testing the limits of existing law and ethical constraints.

Consequently, while the research indicates that state threats have had somewhat mixed effects thus far, this does not guarantee a decline in their use or a lack of impact in the future. Their relative cheapness

---

[41] Kilcullen, D. (2020, pp. 156-157).

[42] Rid, T. (2020, p. 11).

[43] Carson, A., & Yarhi-Milo, K. (2017). Covert communication: The intelligibility and credibility of signaling in secret. *Security Studies 26*(1), 124-156. https://doi.org/10.1080/09636412.2017.1243921

[44] See: Connolly, K. (2024, 11 July). US reportedly foiled Russian plot to kill boss of German arms firm supplying Ukraine. *The Guardian*. https://www.theguardian.com/world/article/2024/jul/11/us-reportedly-foiled-russian-plot-to-kill-boss-of-german-arms-firm-supplying-ukraine; Hancock, A. (2024, 5 April). Russia is trying to sabotage European railways, warns Prague. *The Financial Times*. https://www.ft.com/content/f8207823-f5e1-4caf-934d-67c648f807bf; Kirby, P., & Gardner, F. (2024, 6 November). *Mystery fires were Russian 'test runs' to target cargo flights to US*. BBC News. https://www.bbc.co.uk/news/articles/c07912lxx33o

[45] See: Cybersecurity and Infrastructure Security Agency (CISA). (2024, 7 February). *Cyber security advisory: PRC state-sponsored actors compromise and maintain persistent access to US critical infrastructure*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[46] The term "revisionist states" is taken to mean states that reject the current Western-led, rules-based international system, preferring instead to privilege their own domestic sovereignty and perceived spheres of influence.

[47] Richterova, D., Grossfeld, E., Long, M., & Bury, P. (2024). Russian sabotage in the gig-economy era. *The RUSI Journal*. https://doi.org/10.1080/03071847.2024.2401232

[48] AI is an umbrella term covering various computer technologies used to replicate and improve upon human intelligence; quantum computing is a form of computing that harnesses quantum phenomena to improve processing speed. For examples, see, respectively: Kanade, V. (2022, 4 April). *What is machine learning? Definition, types, applications, and trends*. Spiceworks. https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-ml/; Stryker, C. (2024, 11 October). *Agentic AI: 4 reasons why it's the next big thing in AI research.* IBM. https://www.ibm.com/think/insights/agentic-ai; Stryker, C., & Scappichio, M. (2024, 22 March). *What is generative AI?* IBM. https://www.ibm.com/think/topics/generative-ai; Schneider, J., & Smalley, I. (2024, 5 August). *What is quantum computing?* IBM. https://www.ibm.com/topics/quantum-computing

[49] Smeets, M. (2022, pp. 107-110).

[50] Information operations can involve the spread of disinformation (false material deployed intentionally), misinformation (innocently recycled false material) and malinformation (genuine information never intended for release). See: Omand, D. (2020). *How spies think: Ten lessons in intelligence* (pp. 163-168). Penguin.

and apparent lack of political risk are likely to make them attractive tools of statecraft in the short-to-medium term for various types of states, and their sustained use over time is also likely to have corrosive effects, especially in young democracies or emerging economies that are less well placed to resist them; for example, in regions such as the Balkans and the Sahel.[51] Even highly resilient developed states with robust protections in place may also face greater risks of physical damage or long-term corrosive effects on social cohesion in the face of sustained hostile activity.

Implications

The research does not aim to provide a comprehensive overview of how targeted Western states have responded to various types of state threats, although several initiatives aimed at strengthening economic security, democratic integrity and social cohesion in European and Five Eyes countries are acknowledged. Consequently, the research does not assess the quality and effectiveness of Western responses to the challenge of state threats, nor does it offer detailed policy proposals.[52] However, the research findings hold significant implications for the framing and implementation of future policy for Western governments, which are outlined in five groups of observations below.

Observation 1: Avoid wishful thinking and ignorance when assessing threats and vulnerabilities

In the past 20 years, many Western states have turned a "blind eye" to the hostile actions of states such as Russia and China, prioritising economic relationships and seeing such behaviour as an aberration that can be ignored.[53] Since the full-scale invasion of Ukraine in February 2022, this perspective has changed, although the pronouncements of the recently re-elected US President Donlad Trump suggest the possibility of a less united Western front in the face of Russian aggression at least.[54] The research indicates, however, that regardless of variations in Western policy, the current challenge from state threats will continue. The hostile conduct of states such as Russia, China and Iran, and their use of state threats, reflect their long-term desire to see a world order that rejects liberal rules and norms in favour of hard sovereignty and spheres of influence, within which Western power will be diminished. Unless the US and its allies decide to accept that fate – which seems unlikely, regardless of President Trump's rhetoric – the underlying reasons for conflict will continue. State threats from Russia, China and their associates are unlikely to disappear anytime soon, and may proliferate more widely in their use among non-aligned middle powers and even democratic states. Thus, Western governments must grasp, and continue to acknowledge the significance, dynamics and probable longevity of the challenge.

Western governments must also avoid hubris and overconfidence in their assessment of how well-positioned they are to resist state threats. Open societies present significant attack surfaces for aggressive states.[55] As governments have learned in preparing for disasters, it is perilous to assume that the worst experiences of the past are the right benchmarks for future catastrophes.[56] While Western states have so far not faced major setbacks due to hostile state activity, the possibility that an act of physical sabotage or an offensive cyber operation might have disastrous consequences, including major loss of life, cannot be ruled out. Over the longer term, moreover, the hard-to-detect corrosive effects of persistent hostile activity may indeed begin to surface. If the intensity and potential impact of such activities escalate, current levels of Western resilience and efforts to enhance it may prove insufficient to the task.

To an extent, Western governments are relatively well-placed to understand state threats and their own vulnerabilities because of the high competence and knowledge of their diplomatic cadres, and intelligence and security agencies. Since the terrorist attacks of 11 September 2001 in the US, Western governments have also developed expertise in resilience and protective security. However, in many Western states,

---

[51] On the Balkans, see, for example: Greene, S., Asmolov, G., Fagan, A., Fridman, O., & Guzelov, B. (2021, 23 February). *Mapping fake news and disinformation in the Western Balkans and identifying ways to effectively counter them* [Study requested by the AFET Committee]. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653621/EXPO_STU(2020)653621_EN.pdf. On the Sahel, see: Ersozoglu, E. (2021, 15 April). *Troll-on-troll: Russian-French cyber information war in Africa.* Grey Dynamics. https://greydynamics.com/troll-on-troll-russian-french-cyber-information-war-in-africa/https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653621/EXPO_STU(2020)653621_EN.pdf

[52] These issues require further study; it is hoped that a further opportunity to provide one will be possible in the future.

[53] Fulda, A. (2024). *Germany and China: How entanglement undermines freedom, prosperity and security*. Bloomsbury Publishing; Lough (2021).

[54] Baker, P. (2025, 18 February). Trump's pivot toward Putin's Russia upends generations of US policy. *The New York Times*. https://www.nytimes.com/2025/02/18/us/politics/trump-russia-putin.html

[55] The terms "open" and "closed" societies were coined by French philosopher Henri Bergson in 1932 but are most associated with the work of Austro-British philosopher Sir Karl Popper. Popper saw an open society as individualistic and rationalist in comparison to a collectivist and superstitious alternative of the closed society; see: Hammersley, M. (2024). What is an 'open society'? Bergson, Strauss, Popper, and Deleuze. *History of European Ideas, 50*(8), 1422-1432. https://doi.org/10.1080/01916599.2024.2365143

[56] The experience of rising flood levels in Europe reflects this problem. Flood defences exist but are increasingly inadequate; see: Poynting, M., & Brosnan, G. (2024, 25 September). *Climate change supercharged Europe floods – Scientists*. BBC News. https://www.bbc.co.uk/news/articles/cn5zx2zx5xvo

government departments and agencies are woefully under-resourced in relevant linguistic and cultural expertise or appropriate technical skills. They have, moreover, obvious gaps in their bodies of knowledge and expertise when it comes to understanding more intangible matters such as democratic resilience and social cohesion, or the full spectrum of their countries' vulnerabilities and dependencies on other states, especially complex international systems such as trade, finance, energy supplies and communications infrastructure. If governments are to be able to understand and act upon threats and vulnerabilities, therefore, they must consider whether they have the right people with the right knowledge in place.

Observation 2: Understand opponents' thinking

The research highlights the differing mindsets and worldviews of Russia, China, Iran and North Korea that have allowed them to develop their challenges to the international rules-based order. In all four instances, the strategic cultures of these states show a fluid attitude towards what constitutes peace or war, and an attraction to seeking out loopholes in previously accepted legal frameworks and international norms of behaviour. As Australian scholar-soldier David Kilcullen points out, Russia and China have sought to test the West *vertically* by pushing hostile actions to the threshold of armed conflict and *horizontally* by expanding forms of hostile action across a wide range of areas, many of them unexpected, such as illegal migration.[57] For Western governments and international organisations that emphasise clear legal boundaries and due process, state threats thus pose deep challenges when it comes to framing appropriate and timely responses. Very often, Western governments and organisations simply do not have in place the appropriate structures, processes or capacity to cope.

This suggests that Western countries need to reconsider whether the clear peace/war dichotomy on which they have based their policies for many decades (if not centuries) still makes sense when their opponents are happy to ignore the boundary between them. It further indicates Western countries need to take a more imaginative approach to which sectors threats might emerge from and in what combinations. These suggestions should not be seen as a plea to governments to take an "anything goes" approach or to mindlessly pursue novel potential threats. Legality, and principles of ethics necessity and proportionality, should remain essential to the character of Western responses, as should an ongoing focus on core areas of national security. However, if Western governments do not show more agility, flexibility and creativity in how they respond to state threats, they will risk confirming the assessments of opponents who see them as easy targets, inviting further hostile action.

Observation 3: Ask whether the current resilience-focused model of response is enough

Currently, the core Western approach to state threats is a state-agnostic, resilience-focused model that sometimes seeks to deter or disrupt state threats at source, or use punitive or retaliatory responses – but largely eschews offensive operations and takes a piecemeal approach to developing shared international standards of behaviour. This is especially true in cyberspace, where a strong focus on civilian cyber security has been combined with "persistent engagement" with attackers – a phrase used by cyber scholars Michael Fischerkeller and Richard Harknett.[58] Alongside this, Western powers have also undertaken a desultory diplomatic pursuit of international standards for cyber operations.[59]

Based on the long-term nature of the threat, however, a key question that Western governments need to address is whether the current balance between different types of measures is appropriate. The resilience-based model alone is far from cost-free, and there will be natural and appropriate concerns about the risks of heavy-handed legislation or regulation of fundamental freedoms, whether political, social or economic. The cost of upgrading the resilience of existing systems, structures and processes, or better yet by building it in by design, would need to be explicitly accepted; and, to protect civil liberties, checks and balances on intrusive legislation such as legislative renewals and sunset clauses would need to be considered.

Furthermore, governments must consider whether they are prepared to protect and insulate themselves from hostile actions and more frequently pre-empt attacks, react to them and possibly escalate in response. Western states must carefully evaluate how to alter aggressors' "return on investment" calculations, not only by mitigating the effects of hostile state behaviour, but also by imposing costs that may shift the decision-making processes of perpetrator states. Doing so might

[57] Kilcullen, D. (2020, pp. 175-176).

[58] Fischerkeller, M., & Harknett, R. (2023, pp. 109-133).

[59] Basu, A., Poetranto, I., & Lau, J. (2021, 19 May). The UN struggles to make progress on securing cyberspace. The Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2021/05/the-un-struggles-to-make-progress-on-securing-cyberspace?lang=en; Fischerkeller, M., & Harknett, R. (2023, pp. 109-133).

offer Western governments more opportunities to shape the environment they face.

However, if they choose a more assertive path, they will also need to calibrate how far they are willing to go. Quite apart from triggering a hostile response, such behaviours could have a potentially degrading effect on the West's ideas about itself, its standards and its wider reputation, as the US intelligence community found in the wake of revelations about its past behaviour in the mid-1970s.[60] Were legal and ethical tolerances to change dramatically, and the consequences of these changes to become public, there could be negative effects on public trust in the institutions of government and damage to the reputation of Western states as upholders of international standards, feeding Chinese and Russian narratives, about Western hypocrisy and further undermining the integrity and stability of the rules-based order. If reactive and explicitly offensive measures are to come into play, therefore, they will need to be circumscribed and calibrated within legal and ethical bounds.

To mitigate the accusations that the West is just as bad as its opponents and to create preventative measures against proliferating hostile state behaviours, Western states will also need to consider what they do to shape international standards. Assertive diplomacy in multilateral and "minilateral"[61] forums might kickstart discussions about international standards in non-military conflict, starting with cyberspace, but expanding to cover the role and scope of espionage, sabotage and subversion outside periods of traditionally defined war. Although these are unlikely to gain immediate traction with states such as Russia, Iran or North Korea, they may gain a hearing with a less truculent China and offer a nucleus of consensus that could help provide a barrier to the proliferation of hostile activities in the future.

Observation 4: Shape a coherent, comprehensive and prioritised set of responses

The research highlights the complex and often decentralised nature of how state threats emerge in perpetrator states. Regime objectives are sometimes achieved through top-down direction and at other times via more entrepreneurial initiatives. These regimes have various channels of operational action available to them, including both state agencies and state-linked non-state actors. Western governments must be cognisant of this reality, while also refraining from assuming that an equally diffuse set of countermeasures will be effective in response. In fact, the frequently episodic character and disorienting effect of state threats necessitate that Western governments develop clear and coherent narratives and strategies to avoid losing sight of the significance of these threats.

Western governments therefore need to consider how best to organise their responses, giving particular attention to threats' cross-domain character. This will necessitate a coherent risk assessment and a common strategy across government and society. National governments need to develop a "single point of view" on state threats, and effective leadership and coordination mechanisms to guide and oversee strategic implementation, necessitating closer cooperation between agencies and government departments dealing with different dimensions of the same problem. One such area is tackling the activities of state-linked organised crime, which will require coordination, intelligence sharing, and even joint-working between intelligence agencies and law enforcement.

Prioritisation will also be essential. Countries must carefully assess the full range of threats and vulnerabilities, while pragmatically considering the time and resources available. Not all vulnerabilities can be addressed simultaneously and the order in which they are tackled is significant. In this context, governments may find it tempting to concentrate on familiar areas, as much resilience work will involve the protection of processes, networks, assets and people, most of which will be relatively easy to map and measure. However, governments must also address the more intangible elements of democratic and societal resilience, which are sometimes perceived as overly challenging to tackle but likely pose the greatest existential risks if left unmitigated. Furthermore, governments need to remain vigilant and responsive to emerging threats or vectors of attack. However, they should not unthinkingly pursue novel issues for their own sake, shifting resources en masse at the expense of tackling existing and unmitigated challenges. This is particularly important when considering the potential impact of AI, the promise and dangers of which are far from clear at present.

---

[60] Johnson, L. (2015). *A season of inquiry revisited: The Church Committee confronts America's spy agencies.* University Press of Kansas.

[61] Minilateralism refers to collaboration between small groups of states on specific issues where they have shared interests; see: Mladenov, M. (2023, 14 April). *Minilateralism: a concept that is changing the world order*. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/minilateralism-concept-changing-world-order

Observation 5: Take an approach based on partnership, both domestically and internationally

As the research indicates, in some of the most active perpetrator states, particularly Russia and China, the regimes adopt a whole-of-society approach to executing clandestine and covert activity.[62] Furthermore, although these states do not appear to have established security ties with one another comparable to a Five Eyes-type relationship, there are signs of cooperation in sharing online expertise and evading sanctions, and in the sphere of online disinformation, with states recycling and echoing the narratives of the other revisionist states.[63]

The liberal democratic states of the West cannot aspire to emulate authoritarians' mobilisation of private enterprise and civil society as instruments of the state. Moreover, they should refrain from doing so if they wish to uphold their essential character as open societies. Nevertheless, Western states do not confront a binary choice; the continuum between open and closed societies is wide. As past crises such as the Covid-19 pandemic indicate, liberal democracies can work together in pursuit of broader objectives, temporarily limiting some freedoms without discarding them entirely.

One of the most effective ways to achieve coherence outside of such an obvious crisis is through a partnership model, which may impose some new obligations on the private sector and civil society but will also require willing cooperation, support and initiative from non-governmental actors. The value of this approach has already been observed in areas such as the fight against financial crime, both in the UK and beyond.[64] However, for partnerships to succeed, governments must share a clear threat picture to provide incentives for action, establish a coherent strategy in response and work with non-governmental partners to develop mechanisms for cooperation. In summary, governments need to take businesses, organisations and the wider public into their confidence if they are to address state threats effectively.

Ultimately, the research indicates that the issue of state threats cannot be tackled by a single state in isolation. An international perspective is vital. Many of the threats facing Western states are analogous, as are the vulnerabilities to these dangers. In specific instances, such as the fragility of international infrastructure, these constitute shared challenges.[65] Developing a coherent cross-border response, whether initially through minilateral coalitions of like-minded states or ultimately through broader multilateral platforms such as NATO or the EU, is crucial. Concurrently, the growing risk of the escalating use of state threats by middle powers highlights the necessity for dialogue regarding the perils of persistent hostile activities and their impact on societal resilience and stability. The UN would serve as the obvious platform for this discussion; however, given current divisions within the UN Security Council, more fruitful approaches will likely arise from engagement at bilateral, minilateral and regional levels.

---

[62] Eftiamides, N. (2020); Galeotti, M. (2019, pp. 93-100).

[63] For examples, see: Allen, B. (2023). *Beijing rules: China's quest for global influence* (p. 129). John Murray Press; Azizi, H., & Notte, H. (2024, 14 February). Russia's Dangerous New Friends. How Moscow is Partnering with the Axis of Resistance. *Foreign Affairs*.https://www.foreignaffairs.com/russian-federation/russias-dangerous-new-friends; Fraioli, P. (Ed.). (2023, October). *The surge of activity in relations between North Korea and Russia. Strategic Comments (29)30, International Institute of Strategic Studies.* https://www.iiss.org/globalassets/media-library---content--migration/files/publications/strategic-comments-delta/2023/10/29-30-the-surge-of-activity-in-relations-between-north-korea-and-russia.pdf; Jozwiak, R. (2020, 22 April). EU monitors see coordinated covid-19 disinformation effort by Iran, Russia, China. Radio Free Europe/Radio Liberty. https://www.rferl.org/a/eu-monitors-sees-coordinated-covid-19-disinformation-effort-by-iran-russia-china/30570938.html; Keatinge, T. (2023, June). *Developing bad habits: What Russia might learn from Iran's sanctions evasion* [Occasional paper]. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/occasional-papers/developing-bad-habits-what-russia-might-learn-irans-sanctions-evasion

[64] Maxwell, N.J. (2020, 18 August). *Five years of growth in public–private financial information-sharing partnerships to tackle crime*. Royal United Services Institute Future of Financial Intelligence Sharing Research Programme. https://www.future-fis.com/uploads/3/7/9/4/3794525/five_years_of_growth_of_public-private_partnerships_to_fight_financial_crime_-_18_aug_2021.pdf

[65] Hawker, S. (2023). *Cityforum cyber security summit 2023* (p. 8). Cityforum Limited. https://www.cityforum.co.uk/wp-content/uploads/2023/08/2023-Cyber-Security-Summit-Report.pdf

References

Alexander, K.B. (2015, 3 November). *Prepared statement of Gen (Ret) Keith B. Alexander on the future of warfare before the Senate Armed Services Committee*. US Senate Committee on Armed Services. https://www.armed-services.senate.gov/imo/media/doc/Alexander_11-03-15.pdf

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) Militaire Inlichtingen- en Veiligheidsdienst (MIVD) & Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2022, November). *Threat assessment state sponsored actors 2 (TASA).* https://english.aivd.nl/publications/publications/2023/02/13/threat-assessment-state-sponsored-actors-2-tasa

Allen, B. (2023). *Beijing rules: China's quest for global influence*. John Murray Press.

Australian Security Intelligence Organisation (ASIO). (n.d.). *Recognising hostile intelligence activity*. https://nitro.asio.gov.au/recognising-hostile-intelligence-activity/

Azizi, H., & Notte, H. (2024, 14 February). Russia's Dangerous New Friends. How Moscow is Partnering with the Axis of Resistance. *Foreign Affairs*. https://www.foreignaffairs.com/russian-federation/russias-dangerous-new-friends

Baker, P. (2025, 18 February). Trump's pivot toward Putin's Russia upends generations of US policy. *The New York Times*. https://www.nytimes.com/2025/02/18/us/politics/trump-russia-putin.html

Basu, A., Poetranto, I., & Lau, J. (2021, 19 May). *The UN struggles to make progress on securing cyberspace.* The Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2021/05/the-un-struggles-to-make-progress-on-securing-cyberspace?lang=en

Bradshaw, S., Bailey H., & Howard, P.N. (2021). *Industrialized disinformation: 2020 Global Inventory of Organised Social Media Manipulation* [Working paper 2021.1]. Project on Computational Propaganda, Programme on Democracy & Technology, Oxford Internet Institute. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/cybertroop-report20-draft9.pdf

Braw, E. (2022). *The defender's dilemma: Identifying and deterring gray-zone aggression*. AEI Press.

Carson, A., & Yarhi-Milo, K. (2017). Covert communication: The intelligibility and credibility of signaling in secret. *Security Studies 26*(1), 124-156. https://doi.org/10.1080/09636412.2017.1243921

Casciani, D. (2023, 16 February). *Hostile-state threat probes grown fourfold – police.* BBC News. https://www.bbc.co.uk/news/uk-64668063

Cecco, L. (2024, 5 April). India and Pakistan tried to meddle in Canada elections, spy agency says. *The Guardian*. https://www.theguardian.com/world/2024/apr/05/india-pakistan-interfere-canada-elections

Center for Strategic and International Studies (CSIS). (n.d.). *Survey of Chinese espionage in the United States since 2000* [Data set]. https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000

Chainalysis. (2024, February). *The 2024 crypto crime report.* https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf

Chotiner, I. (2020, 23 January). How Putin controls Russia. *The New Yorker*. https://www.newyorker.com/news/q-and-a/how-putin-controls-russia

Connolly, K. (2024, 11 July). US reportedly foiled Russian plot to kill boss of German arms firm supplying Ukraine. *The Guardian*. https://www.theguardian.com/world/article/2024/jul/11/us-reportedly-foiled-russian-plot-to-kill-boss-of-german-arms-firm-supplying-ukraine

Contessi, N. (2016). Prospects for the accommodation of a resurgent Russia. In Paul, T.V. (Ed.), *Accommodating rising powers: Past, present, and future* (pp. 268-289). Cambridge University Press.

Cormac, R. (2022). *How to stage a coup and ten other lessons from the world of secret statecraft*. Atlantic Books.

Council on Foreign Relations (CFR). (n.d.). *Cyber operations tracker* [Data set]. https://www.cfr.org/cyber-operations/

Cybersecurity and Infrastructure Security Agency (CISA). (2024, 7 February). *Cyber security advisory: PRC state-sponsored actors compromise and maintain persistent access to US critical infrastructure*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Daugherty, W.J. (2010). Covert action: Strengths and weaknesses. In L.K. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 608-625). Oxford University Press.

David, M., & D., L. (2024). Russia's war on Ukraine: Unbottled emotions and the conditioning of the EU's Russia policy. *Journal of European Integration 46*(5), 661-684. https://doi.org/10.1080/07036337.2024.2363613

Dowden, O. (2024, 25 March). Cyber security and UK democracy. *Hansard*. UK Parliament. https://hansard.parliament.uk/commons/2024-03-25/debates/096EB6E9-21A1-40A5-A7F4-247C52AFC070/Cyber-SecurityAndUKDemocracy

Dunlap, Jr, C.J. (2001, 29 November). *Law and military interventions: Preserving humanitarian values in 21st century conflicts* [Conference paper]. Humanitarian Challenges in Military Intervention Conference, Carr Center for Human Rights Policy Kennedy School of Government, Harvard University Washington, DC. https://people.duke.edu/~pfeaver/dunlap.pdf

Economy, E.C. (2023). *The world according to China*. Polity Press.

Eftiamides, N. (2020). *Chinese espionage: Operations and tactics*. Vitruvian Press.

Elliott, D. (2024, 26 January). *Middle powers: What are they and why do they matter?* World Economic Forum. https://www.weforum.org/stories/2024/01/middle-powers-multilateralism-international-relations/

Ellis-Peterson, H., Hassan, A., & Baloch, S.M. (2024, 4 April). Indian government ordered killings in Pakistan, intelligence officials claim. *The Guardian.* https://www.theguardian.com/world/2024/apr/04/indian-government-assassination-allegations-pakistan-intelligence-officials#:~:text=The%20majority%20of%20those%20allegedly,which%20have%20killed%20hundreds%20of

Ersozoglu, E. (2021, 15 April). *Troll-on-troll: Russian-French cyber information war in Africa.* Grey Dynamics. https://greydynamics.com/troll-on-troll-russian-french-cyber-information-war-in-africa/

Fischerkeller, M., & Harknett, R. (2023). Cyber persistence, intelligence contests, and strategic competition. In R. Chesney & M. Smeets (Eds.), *Deter, disrupt, or deceive: Assessing cyber conflict as an intelligence contest* (pp. 109-133). Georgetown University Press.

Fraioli, P. (Ed.). (2023, October). The surge of activity in relations between North Korea and Russia. *Strategic Comments (29)*30, International Institute of Strategic Studies. https://www.iiss.org/globalassets/media-library---content--migration/files/publications/strategic-comments-delta/2023/10/29-30-the-surge-of-activity-in-relations-between-north-korea-and-russia.pdf

Freedman, L. (2017). *The future of war: A history*. Penguin Books.

Freeman, B. (2021, 27 July). *Hold the UAE accountable for meddling in US politics.* Defense One. https://www.defenseone.com/ideas/2021/07/hold-uae-accountable-meddling-us-politics/184052/

Fulda, A. (2024). *Germany and China: How entanglement undermines freedom, prosperity and security*. Bloomsbury Publishing.

Galeotti, M. (2019). *Russian political war: Moving beyond the hybrid.* Routledge.

Galeotti, M. (2022). *The weaponisation of everything: A field guide to the new way of war*. Yale University Press.

Giles, K. (2019). *Moscow rules: What drives Russia to confront the West*. Royal Institute of International Affairs.

Giles, K. (2023). *Russia's war on everybody – And what it means for you*. Bloomsbury Publishing.

Greene, S., Asmolov, G., Fagan, A., Fridman, O., & Guzelov, B. (2021, 23 February). *Mapping fake news and disinformation in the Western Balkans and identifying ways to effectively counter them* [Study requested by the AFET Committee]. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653621/EXPO_STU(2020)653621_EN.pdf

Greitens, S.C. (2014). *Illicit: North Korea's evolving operations to earn hard currency*. Committee for Human Rights in North Korea. https://www.hrnk.org/documentations/illicit-north-koreas-evolving-operations-to-earn-hard-currency/

Hammersley, M. (2024). What is an 'open society'? Bergson, Strauss, Popper, and Deleuze. *History of European Ideas, 50*(8), 1422-1432. https://doi.org/10.1080/01916599.2024.2365143

Hancock, A. (2024, 5 April). Russia is trying to sabotage European railways, warns Prague. *The Financial Times*. https://www.ft.com/content/f8207823-f5e1-4caf-934d-67c648f807bf

Hawker, S. (2023). *Cityforum cyber security summit 2023.* Cityforum Limited. https://www.cityforum.co.uk/wp-content/uploads/2023/08/2023-Cyber-Security-Summit-Report.pdf

Home Office. (2021, 13 May). *Legislation to counter state threats (hostile state activity)* [Government consultation]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986013/Consultation_Document_-_Legislation_to_Counter_State_Threats.pdf

Hybrid Center of Excellence (Hybrid CoE). (n.d.). *Hybrid threats as a concept.* https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Johnson, L. (2015). *A season of inquiry revisited: The Church Committee confronts America's spy agencies.* University Press of Kansas.

Jones, S.G. (2023). Soleimani, Gerasimov, and strategies of irregular warfare. In H. Brands (Ed.), *The new makers of modern strategy: From the ancient world to the digital age* (pp. 996-1021). Princeton University Press.

Joske, A. (2022). *Spies and lies: How China's greatest covert operations fooled the world*. Hardie Grant Books.

Jozwiak, R. (2020, 22 April). *EU monitors see coordinated covid-19 disinformation effort by Iran, Russia, China*. Radio Free Europe/Radio Liberty. https://www.rferl.org/a/eu-monitors-sees-coordinated-covid-19-disinformation-effort-by-iran-russia-china/30570938.html

Kanade, V. (2022, 4 April). *What is machine learning? Definition, types, applications, and trends*. Spiceworks. https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-ml/

Keatinge, T. (2023, June). *Developing bad habits: What Russia might learn from Iran's sanctions evasion* [Occasional paper]. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/occasional-papers/developing-bad-habits-what-russia-might-learn-irans-sanctions-evasion

Kilcullen, D. (2020). *The dragons and the snakes: How the rest learned to fight the West*. Hurst & Company.

Kirby, P., & Gardner, F. (2024, 6 November). *Mystery fires were Russian 'test runs' to target cargo flights to US*. BBC News. https://www.bbc.co.uk/news/articles/c07912lxx33o

Krastev, I. (2022, 18 November). Opinion: Middle powers are reshaping geopolitics. *The Financial Times*. https://www.ft.com/content/0129492d-ac7f-4807-8050-2760a09e9ccc

Krieg, A. (2023). *Subversion: The strategic weaponization of narratives.* Georgetown University Press.

Lewis, D.G. (2020). *Russia's new authoritarianism: Putin and the politics of order*. Edinburgh University Press.

Lough, J. (2021). *Germany's Russia problem: The struggle for balance in Europe*. Manchester University Press.

Mackintosh, T. (2024, 3 April). *Pouria Zeraati: Three accused of TV presenter attack have left UK*. BBC News. https://www.bbc.co.uk/news/uk-england-london-68717210

Maness, R.C., Valeriano, B., Hedgecock, K., Macias, J.M., & Jensen, B. (2023). Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID): Cyber conflict from 2000-2020, *The Cyber Defense Review, 8*(2), 65-89. https://cyberdefensereview.army.mil/Portals/6/Documents/2023_Summer/Maness_Macias%20et%20al%20CDR%20V8N2%20Summer%202023.pdf?ver=iJDHRpDvaq-hW4Zde6EwUg%3d%3d

Martin, P. (2021). *China's civilian army: The making of wolf warrior diplomacy.* Oxford University Press.

Maschmeyer, L. (2021). The subversive trilemma: Why cyber operations fall short of expectations. *International Security 46*(2), 51-90. http://dx.doi.org/10.1162/isec_a_00418

Maxwell, N.J. (2020, 18 August). *Five years of growth in public–private financial information-sharing partnerships to tackle crime*. Royal United Services Institute Future of Financial Intelligence Sharing Research Programme. https://www.future-fis.com/uploads/3/7/9/4/3794525/five_years_of_growth_of_public-private_partnerships_to_fight_financial_crime_-_18_aug_2021.pdf

McCallum, K. (2022, 16 November). *Annual threat update* [Transcript]. MI5. https://www.mi5.gov.uk/news/director-general-ken-mccallum-gives-annual-threat-update

Mladenov, M. (2023, 14 April). *Minilateralism: A concept that is changing the world order*. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/minilateralism-concept-changing-world-order

Nakamura, R., & Kobara, J. (2023). *'North Korea gets half its foreign currency from cyber theft': US official.* Nikkei Asia. https://asia.nikkei.com/Spotlight/N-Korea-at-crossroads/North-Korea-gets-half-its-foreign-currency-from-cyber-theft-U.S.-official#:~:text=North%20Korea%20gets%20half%20its%20foreign%20currency%20from%20cyber%20theft%3A%20U.S.%20official,-Washington%20seeks%20clampdown&text=SINGAPORE%20%2D%2D%20The%20U.S.%20estimates,senior%20American%20official%20told%20Nikkei

Omand, D. (2020). *How spies think: Ten lessons in intelligence* (pp. 163-168). Penguin.

Paul, T.V. (2016). The accommodation of rising powers in world politics. In T.V. Paul (Ed.), *Accommodating rising powers: Past, present, and future* (pp. 3-32). Cambridge University Press.

Poynting, M., & Brosnan, G. (2024, 25 September). *Climate change supercharged Europe floods – Scientists*. BBC News. https://www.bbc.co.uk/news/articles/cn5zx2zx5xvo

Public Safety Canada. (2022, 25 April). *Parliamentary committee notes: Countering hostile activities by state actors*. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20220930/06-en.aspx

Rathbone, J.P., & Reed, J. (2023, 20 September). India's foreign spy agency drawn out of the shadows by Canadian allegations. *The Financial Times*. https://www.ft.com/content/764a8989-ceac-4fff-85db-bc130f913f82

Rathbone, J.P., & Reed, J. (2024, 14 May). China poses 'genuine and increasing cyber risk' to UK, warns GCHQ head. *The Financial Times*. https://www.ft.com/content/22249735-29ed-4902-8a43-482943ae3323

Reimer, S., & Redhead, M. (2021, May). *A new normal: Countering the financing of self-activating terrorism in Europe* [Occasional paper]. Royal United Services Institute. https://static.rusi.org/265_op_lone_actor_0.pdf

Richterova, D., Grossfeld, E., Long, M., & Bury, P. (2024). Russian sabotage in the gig-economy era. The RUSI Journal. https://doi.org/10.1080/03071847.2024.2401232

Rid, T. (2017). *Cyber war will not take place*. Oxford University Press.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Profile Books.

Riehle, K. (2022). *Russian intelligence: A case-based study of Russian services and missions past and present.* National Intelligence University, United States Government.

Riehle, K.P. (2024). Ignorance, indifference, or incompetence: Why are Russian covert actions so easily unmasked? *Intelligence and National Security 39*(5), 864-878. https://doi.org/10.1080/02684527.2023.2300165

Royal United Services Institute (RUSI). (n.d.). *RUSI State Threats Taskforce (STT).* https://rusi.org/explore-our-research/projects/rusi-state-threats-taskforce-stt

Royal United Services Institute (RUSI). (2023a, March). *State Threats Taskforce: 'Assessing the threats'* [Conference report]. https://static.rusi.org/393-CR-SST-Meeting-One-State-Threats-web-final-updated.pdf

Royal United Services Institute (RUSI). (2023b, June). *State Threats Taskforce: 'Assessing the responses'* [Conference report]. https://www.rusi.org/explore-our-research/publications/conference-reports/rusi-state-threats-taskforce-assessing-responses

Sandford, D. (2024, 26 April). *Two British men charged with helping Russian intelligence*. BBC News. https://www.bbc.co.uk/news/uk-68899130.

Schneider, J., & Smalley, I. (2024, 5 August). *What is quantum computing?* IBM. https://www.ibm.com/topics/quantum-computing

Smeets, M. (2022). *No shortcuts: Why states struggle to develop a military cyber-force*. Hurst & Company.

Stryker, C. (2024, 11 October). *Agentic AI: 4 reasons why it's the next big thing in AI research.* IBM. https://www.ibm.com/think/insights/agentic-ai

Stryker, C., & Scappichio, M. (2024, 22 March). *What is generative AI?* IBM. https://www.ibm.com/think/topics/generative-ai

Suzuki, S. (2017). 'Delinquent gangs' in the international system hierarchy. In A. Zarakol (Ed.), *Hierarchies in world politics* (pp. 219-240). Cambridge University Press.

Tsang, S., & Cheung, O. (2024). *The political thought of Xi Jinping*. Oxford University Press.

White, G. (2022). *The Lazarus heist: From Hollywood to high finance: Inside North Korea's global cyber war*. Penguin.

Wray, C. (2020). *The threat posed by the Chinese government and the Chinese Communist Party to the economic and national security of the United States* [Transcript]. Federal Bureau of Investigation. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

About SOC ACE

The Serious Organised Crime & Anti-Corruption Evidence (SOC ACE) research programme aims to help 'unlock the black box of political will' for tackling serious organised crime, illicit finance and transnational corruption through research that informs politically feasible, technically sound interventions and strategies. SOC ACE is funded by the UK Foreign, Commonwealth & Development Office, and is led by Professor Heather Marquette at the University of Birmingham, working in collaboration with a number of leading research organisations and through consultation and engagement with key stakeholders. The views expressed here do not necessarily reflect the UK Government's official policies.

Find out more

www.socace-research.org.uk

Follow us on Blue Sky: @soc-ace.bsky.social

Follow us on LinkedIn: @socace-research

SOC ACE | University of Birmingham | Birmingham| B15 2TT | United Kingdom

UNIVERSITY OF BIRMINGHAM

UK Government

RUSI

If you've used this research to inform your work,
let us know by sending us an email to: **impact-socace@contacts.bham.ac.uk**