Findings of a Round-Table in support of the Secretary of State's Office of Net Assessment and Challenge (SONAC), Ministry of Defence

Brunel Centre for Intelligence & Security Studies (BCISS)

Brunel University London

14 Apr 2023

Participants

Brunel University

- Prof Philip H.J. Davies
- Dr. Neveen S. Abdalla
- Dr. Kristian Gustafson (Chair)
- Dr. Dan Lomas
- Dr. Steven Wagner

Guest Panellists

- Dr. Matthew Ford, Associate Professor, Swedish Defence University
- Mr. Jim Green, Prevail Partners Ltd
- Ms. Elena Grossfeld, PhD Candidate, War Studies, King's College London
- Dr. Louise Kettle, Assistant Professor, University of Nottingham
- Maj Gen (Ret) Ben Kite, Kearney
- Ms. Magda Long, PhD Candidate, War Studies, King's College London
- Dr. Dennis Molinaro, OntarioTech University, Canada
- Dr. Lynette Nusbacher, Devil's Advocate, Nusbacher & Associates Ltd
- Dr. Mark Stout, Johns Hopkins University (Retired)

SONAC Representative

- Dr. Benedict Docherty

Recorders:

- Ms. Eva Tautkute, BCISS
- Mr. Sean Sarfas, BCISS

Key

Issue

1. Dr Rob Johnson, Director of the Secretary of State's Office of Net Assessment and Challenge (SONAC) invited the Brunel Centre for Intelligence & security Studies (BCISS) to inform the next Defence Command Paper by convening a round-table of academic and private sector experts on defence issues. The aim is to help shape the future direction of UK Defence and the Integrated Review (Refresh) by answering questions set by SONAC. The round-table was conducted on 11 April 2023, and this report prepared for submission on 14 Apr 2023.

Agenda & Methods

2. The following report captures key themes and conclusions arising from a roundtable discussion conducted by the Brunel Centre for Intelligence and Security Studies (BCISS) and colleagues from around the world, on behalf of the Secretary of State's Office of Net Assessment and Challenge (SONAC). The purpose of the roundtable was to contribute to informing the planned Defence White Paper by focusing *specifically* on key and emerging intelligence issues and developments.

3. Historically regarded as a 'handmaiden to policy' and to operations, intelligence has progressively taken an increasingly significant role in every aspect of national security and defence. This has been driven chiefly by three things:

a. The centrality of 'intelligence, surveillance and reconnaissance' (ISR) in high-tech conflict shaped by network-enabled capabilities and smart munitions;

b. The linchpin role of intelligence in counterterrorism and counterinsurgency; and most recently

c. The immediacy and impact of a renewed level of threat from global actors like Russia and the People's Republic of China.

4. Intelligence has recently even been elevated to the status of a Defence 'Function,' that is, an activity that must be delivered 'in a coherent way across all the organisations in Defence.' Nonetheless, the UK might profitably consider the example of Singapore, a small but capable regional power, that has even amalgamated its defence cyber and intelligence components into a new Service Branch, the Digital and Intelligence Service (DIS) on a footing equal to its Army, Navy, and Air Force.

5. In our discussion we have *not* approached 'intelligence' in its narrow, military doctrinal sense of information to support command decision-making, or through the constrictive conventions of the so-called 'intelligence cycle.' We have, rather, employed Roy Godson's 'elements of intelligence' taxonomy of 'what intelligence agencies do' that includes:

a. Intelligence Collection
b. Intelligence Analysis
c. Counterintelligence
d. Covert Action

6. 'Covert action,' of course, is the term employed when we and our allies pursue conflict and confrontation through other, clandestine means. When the same activities are undertaken by rivals, adversaries, and enemies they appear under different, more pejorative names like *sabotage* and *subversion*, influence, information, and disinformation operations. And, of course, detecting, penetrating, and preventing adversary covert action along with countering their espionage is a core mission of counterintelligence. Intelligence, therefore, must have its own 'integrated approach' as much as wider Defence and Government. That integrated approach to intelligence is the principal theme of this report.

7. **Method:** This panel consisted of a mix of 14 academic and professional individuals, all expert in aspects of the key question set. It was conducted online. Each of the six headline questions set by SONAC was given 15-20 minutes of discussion time. The panel was chaired, but discussion was guided by the varied individual expertise and contributions.

8. The panel proceeded without disagreement on key points. Accordingly, the findings are presented without direct reference to individual speakers. We present all comments as derived from the panel as a single body. SONAC staff were observers only and did not contribute to or steer discussion in any way.

Question 1: What priority problems and key threats do we want to address over the next ten years?

9. **For intelligence, the question of priority problems is very much that of the problem with priorities**. Successive reviews of intelligence failure, both in strategic warning and counterterrorism, have found that the necessity of prioritising targets and lines of investigation often creates the points of vulnerability where warning fails and attacks take place. Historical analysis of attempts to forecast the future shape of warfare has also suggested that too often forecasters prioritise technological

innovation over human factors such as the volatility of alliances and strategic alignments. It is essential, therefore, to be clear that forecasting the origins or actors from which threats originate is a very different problem from predicting the vectors or shape those threats will take when implemented. However, the latter will inevitably shape the former to a significant degree.

10. **The panel largely accepted the premise that Russia and China were the principal threat actors in coming decades from the UK perspective. But, each drives very different threat vectors.** China represents the more radical shift in the threat environment. This is partly because of scale but mainly because China's pursuit of dominance in key emerging technologies such as artificial intelligence (AI) and quantum computing imply very different potential threat vectors from other states, and at very different levels. The most intuitive of these transformations in kinetic threats at the tactical and operational levels from AI-controlled swarms of uncrewed systems that increase agility and accelerate the user's decision cycle. A far more profound shift is presented by the degree to which international competition shifts to a technological competition and economic competition that will decide which geopolitical players will hold the necessary technological advantages.

11. **Economic and Politico-Military Blocs are becoming indistinguishable.** In this context, developments like the PRC's belt-and-road initiative become strategic positioning enterprises, creating alliances of economic alignment and dependence amongst states that the West has difficulty cultivating. Technology acquisition, whether overt, clandestine, or merely concealed by arcane layers of corporate ownership and investment becomes a collective as well as UK national security issue. While scientific and technological espionage may have been Soviet stock in trade during the Cold War, China represents a step change in this type of threat. The Russian 'special services' have attracted the most public attention in the last two decades as much for their paramilitary activities as for espionage and cyber information operations. China, however, has been resourcing its offensive human intelligence (HUMINT) effort, especially through the Ministry of State Security (MSS), on an unprecedented scale. There is also an extensive 'grey' effort at acquiring Western technical know-how through investment in UK and allied research development programmes. China is also engaged in extensive clandestine and 'grey' efforts to interfere in public institutions and policy-making to favour its industrial-technological interests.

12. **The most significant change in intelligence priorities in the next decade therefore will be the increased significance of counterintelligence.** The most striking transformation in intelligence priorities currently is, therefore, a renewed emphasis on *counterintelligence*, covering countersubversion (influence) and countersabotage as well as counterespionage. Since the Cold War, counterintelligence has become something of a backwater nationally and in Defence, supplanted in priorities and influence by counterterrorism and counterinsurgency. This is no longer tenable. The scale of Chinese and Russian espionage efforts has reduced CI to a frustrating exercise in 'whack-a-mole' in which insider threat detection is always going to be a step behind. Perhaps the most important counterintelligence lesson from both the Second World War and Cold War was that effective counterintelligence depends upon successful intelligence penetration of the adversaries' own intelligence operations. This can illuminate their operations, but also a broader strategic picture of how they target us. Reforms to Defence counterintelligence since 2014 have strengthened that activity, but it remains seriously underdeveloped compared to the diversity and level of threat.

13. **Loss of technical and other information advantages implies the loss of economic competitive advantages.** Industrial and technological competition represents a renewed threat context at the level of macroeconomic competition. Developing, acquiring, and deploying Defence and other

national security capabilities depends fundamentally on economic prosperity. Under both the *Security Service Act 1989* and *Intelligence Services Act 1994* the UK's Security and Intelligence Agencies have a statutory mandate to operate in support of the UK's 'economic wellbeing'. The relationship between Defence Intelligence and 'economic wellbeing', however, is more one of dependence than guardianship. Defence counterintelligence is particularly close to this problem because of the importance of counterintelligence competence in the industrial and technological supply chains. Consequently, counterintelligence needs to be seen as integral to intelligence as a Defence 'Function' as intelligence production to support decision-making and understanding.

Question 2: How have the threats changed, and how could they change further?

14. **The threat environment is dynamic and always has been.** We note that it is the technological drivers of that change which attract the most public attention, but that it is socio-economic and socio-political issues which in fact generate much of those shifts.[1] It is important for the UK to recognise its place in the world and the shifting currents around it: there is a clear change in position of UK in strategic global order. In *absolute terms* we are not losing ground or getting weaker, but the world is becoming more equal. More equal does not mean more friendly or more aligned in interests. That increasing equality increased the number of actors, both state and non-state, who may become threats to our interests. More capabilities are being affordable for more actors. There is a levelling of the field for global strategy and politics, a fact we need to recognise with clear eyes.

15. **HFS will try to erode UK alliances and relationships, and this may see new combinations of threat in unexpected areas.** China and Argentina have recently been visibly courting one another. China is seeking to cultivate allies and satellites in Latin America and secure food and fuel supply chains from the region. Argentina is seeking a major power sponsor for its territorial claims in the South Atlantic, and a means to by-pass the UK's perceived blockade on Argentinian arms purchases from Western suppliers. At the same time, Commonwealth member and putative ally, or at least friendly state, South Africa has been cultivating closer defence relations with Russia concurrently with the latter's invasion of Ukraine. Such permutations and combinations of threat actors means that intelligence must be especially agile and try to minimise the geographical and functional stovepiping of intelligence collection, analysis and counterintelligence investigation.

16. **The global strategic environment is an increasingly level playing field: The UK must change its mindset.** The power gap between nominally major powers and smaller players has been consistently narrowing at least since the 1980s, and the entry costs for acquiring peer-level capabilities have been falling for at least as long. The UK cannot, therefore, assume it will always retain the initiative and a position of technological superiority. More "insurgent thinking" is required.

17. **Space is a key capability/vulnerability raised by the panel.** The cost of accessing space for communications, earth observation, SIGINT and other purposes is now much lower, allowing more players to access it. Where before Five Eyes (FVEY) and Western Allies had a near monopoly on space for intelligence and defence purposes, it is now a domain in which the UK operates at risk: space is now both an asset and a vulnerability to the UK. All nations will begin to fear other nations interfering with their access to space, and this sense of having sovereignty in space infringed upon will become a flashpoint.

[1] Lawrence Freedman, *The Future of War: A History*. London: Allen Layne, 2017.

18. **We need to incorporate space domain awareness into the lexicon of intelligence, and similarly, our awareness of the adversary space domain awareness.** Space is now more than just a collection vector for us: it is an arena in which we need to develop domain awareness, and a venue into which our counterintelligence enterprise must expand.

19. **Large, open-source data sets, what the panel called "data democracy" or the increasing availability of data to everyone, is another critical driver**. The barriers to entry into very rich open-source intelligence are extremely low. Any actor with modest resources can buy satellite data, or data derived from satellites at competitive prices. Previously this would have been restricted solely to major states. These capabilities stretch close to ubiquitous technical surveillance. It is deeply worrying that such a wide range of state actors or non-state actors could exploit large data sets for intelligence purposes, developing Insights into our organisations and identifying access points. It is a deeply worrying trend, which we think we will see grow more in the next five years paired with increasing availability from cloud or processing capabilities to extract value from those big data sets.

20. **The availability of data is accelerating as data sensors are everywhere now.** Everyone carries a very sophisticated sensor for sound, images and locations in their pockets all the time with their mobile phones. With billions of these devices, and their data pull captured by state and commercial actors, there is thus very large amounts of rich data which we can exploit—and which can be exploited against us. This exploitation can happen across all levels of warfare: tactical, operational, and strategic. The implications of this for the MOD are (a) the need to use commercial partners to help access this data, (b) the need to provide the analytical capability to derive intelligence value from it at often very low levels of military organisation and (c) the need to apply counterintelligence capabilities and security measure to mitigate and secure against own flood of data into the open source from the capabilities listed above.

Question 3: What is the best way that UK Defence could contribute to facing the 'epoch-defining challenge of China'?

21. **The panel notes that discourse on UK Defence contribution requires recognition that China's views on warfare and competitiveness are much more integrated than in the UK.** The PRC utilises a "Total Cold War" approach, wherein China's competitiveness includes all levels and instruments of national power. Chinese non-state actors, corporate entities, and individual researchers, engage in intelligence collection and the gathering of intellectual property. The Chinese diaspora can engage in collection and influence operations, reducing counterintelligence efforts to a game of "whack-a-mole", consistently trying to stop the next insider threat from developing. In addition to vast intelligence collection resources, and significant SIGINT and Cyber capabilities, the PRC also has access to, or control of, strategic physical assets globally. This includes ports, industrial facilities, and mines. They are also making inroads in third countries that the UK government may have previously presumed "safe".

22. **Chinese activities pose a direct threat to the MOD and UK national interests**. This is seen in PRC support for Argentina's oil claims against the Falklands, and in Chinese control of many critical mineral markets. China's mineral export restrictions make UK industries susceptible to market shocks,

geopolitical events, logistical disruptions or supply chain interdictions.[2] The panel observes that China could potentially leverage its Export Control Law of October 2020 to weaponize logistics.[3] Given Beijing's close ties with Russia, weaponization of the supply chain could negatively impact the UK and other states that support Ukraine.

23. **UK universities are at risk of falling prey to Chinese economic incentives.** China has capitalized on filling the void of funding, making sweetheart offers to academics or departments. For example, Sussex University is one of a few institutions in the UK that has quantum computers. To address the lack of funding to maintain its programme, they have entered an agreement with Zhejiang Gongshang University in China to provide teaching courses in AI.[4] Similar efforts are seen across the FVEY. Often the research resulting from these partnerships directly feeds into the civil-military fusion structure of the PRC. This raises broader question of how to secure UK academic institutions.

24. **The panel highlights a disconnect of views within the UK, where China is simultaneously seen as a security threat and an investment opportunity.** These disparate perceptions engender hesitance to take direct action to protect UK interests. Members of the panel voice concern that PRC will not be treated as a threat until a hard-power event (i.e., an invasion of Taiwan) appears imminent. Recent precedent exists with Russia, where the invasion of Ukraine spurred an impetus for the UK Government to crack down on long-known Russian illicit money and intelligence operations.

25. **PRC is a "hard target", and gathering intelligence necessitates use of similar tactics against them, while simultaneously shoring up UK hard-target capacities.** This includes harnessing business, corporate, and research angles to understand the PRC and their intelligence requirements. The panel notes that similar relationships exist between the US government relationship and private corporations. Deeper knowledge of PRC agreements would provide substantial direction for counter-influence operations, providing the dual benefits of thwarting Chinese influence while countering with equally enticing agreements to third nations.

26. **There is an absence of offensive information operations against the PRC.** The lack of attention and resources in counterintelligence, conditioned by our focus on Iraq and Afghanistan, needs to be reversed. Much of the current response is geared toward countering malign actors or information operations, but detecting inside threats is insufficient. The threat from China merits a proactive counter-espionage effort, rather than just a defensive counterintelligence effort. The panel observes that while have seen defectors from Russian agencies, there is no visible equivalent occurring Chinese agencies, nor is there evidence of successful penetration efforts. Further, financial intelligence (FININT), including network analysis to identify both licit and illicit transfers of money.

27. **The challenge of China also brings opportunity for the UK intelligence community.** It is an opportunity to reconsider the ability to meet the information revolution and other changes which have happened in the last 20 years. China, as a strategic mission, allows for long-term focus and offers

[2] United Kingdom Department for Business and Trade. (2023). *Resilience for the Future: The UK's Critical Minerals Strategy*. [online] Available at: https://www.gov.uk/government/publications/uk-critical-mineral-strategy/resilience-for-the-future-the-uks-critical-minerals-strategy#what-is-a-critical-mineral [Accessed 13 Apr. 2023].

[3] National People's Congress of the People's Republic of China. (2020). *Export Control Law of the People's Republic of China*. [online] Available at: http://www.npc.gov.cn/englishnpc/c23934/202112/63aff482fece44a591b45810fa2c25c4.shtml [Accessed 13 Apr. 2023].

[4] Sussex University. (n.d.). Sussex Artificial Intelligence Institute, Zhejiang Gongshang University : Partnership engagement : ... : Global engagement : University of Sussex. [online] Available at: https://www.sussex.ac.uk/global-engagement/partnerships/engagement/sussex-artificial-intelligence-institute [Accessed 13 Apr. 2023].

cross-government opportunities to work together using the fusion doctrine. From strategic to tactical levels, the China challenge can bring together the MOD, FCDO, and other core groups, alongside academia and commercial entities. It is an opportunity to look at how intelligence of the future should be. A defensive front that includes the UK private tech sector will be beneficial, as many of the problems posed by China can be addressed when the industry works in collaboration with the UK Government. It is important to overcome reluctance or barriers that prevent cooperation between the public and private sectors.

Question 4: Can the UK be protected by Defence from air strikes, space attack, or supply chain interdiction, and, if not, what must it do?

28. **Warning Intelligence is the first line of defence against any form of attack in any domain, land, air, maritime or space, whether kinetic, cyber or economic.** While intelligence on adversary systems and capabilities is vital to crafting defences against them, the crucial intelligence issue here is that of *indicators and warning* (I&W). Warning intelligence traditionally has the reputation of being the class of intelligence activity most likely to fail, or at least fail visibly.[5] By contrast, the Ukraine conflict will likely prove a seminal lesson in what timely and accurate warning can achieve. The panel identified several additional issues arising from the need for effective, accurate and robust I&W:

a. Space, Intelligence and Counterintelligence
    a. The Internet of Things (IoT) as Intelligence Source
    b. AI automation and enhancement of I&W.
    c. Economic Warfare
    d. Human Factors and Understanding

29. ***Space, Intelligence and Counterintelligence:*** **Space domain awareness (SDA) is treated as an activity entirely separate from intelligence. This is an artificial and dangerous separation.**

a. SDA is a vital ingredient of both situational awareness and intelligence preparation of the environment (IPOE) through indications generated by hostile space activity.

b. SDA requires all-source intelligence approach and should be aligned with, or integrated into, the intelligence Function. It employs a multi-disciplinary combination of space surveillance radars, ground- and space-based telescopes, monitoring signal traffic between space assets and ground-based controllers, and inferences about a satellite's mission and capabilities drawn from e.g. its orbital inclination and altitude.

c. Finally, assessment of adversaries' space reconnaissance capabilities and assessing the vulnerability of friendly forces to those capabilities is, essentially, a form of battlespace counterintelligence. While Russian optical and synthetic aperture capabilities are much diminished since the Cold War, China has been investing heavily in this area. Many nominally smaller powers also now have access to limited sovereign capabilities as well as the near-global, near-real time coverage offered by commercial services like Maxar and public Earth Observation services like the EU's Sentinel constellation.

[5] See, e.g. Michael Herman *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996) 227,233-234.

30. ***Internet of Things (IoT) as Intelligence Source:*** **Logistical information is often vital to I&W, but the IoT promises to generate unprecedented and seemingly intractable volumes of information for intelligence exploitation**. This, in turn, leads to the question of the (at least partial) automation of IoT exploitation. Entirely new types of real- and near-real time SIGINT will become available as vehicles, transport infrastructure and devices such as smart fridges carrying perishable medical supplies, plus wearable and implantable technologies all communicate with one another wirelessly and, from the user's perspective, transparently. This offers a trove of intelligence and especially warning intelligence, but at the same time we must consider the counterintelligence and operations security angles of limiting an adversary's ability to exploit our own IoT traffic.

31. ***AI and Automation:*** **I&W is naturally amenable to increased automation through AI but the trends discussed make this a mandatory line of development**. The basic nature of matching indications against warning criteria is an activity suitable to some of the most basic and long-established AI techniques. In a complex, fluid international arena increasingly shaped by numerous, agile and often dispersed systems acting across multiple domains the volume of data being reported by collection systems will increasingly outstrip human cognition. This will be intensified by the IoT.

32. ***Economic Warfare:*** **It was agreed that the supply chain issue raises a wider concern about economic warfare, and especially economic sabotage**. This presents a range of intelligence challenges, such as the ability to detect economic disruption and sabotage, especially if:

a. conducted incrementally over time;
b. directed at localised or sector-specific vulnerabilities;
c. implemented conducted through proxies such as independent commercial concerns, possibly in third countries, and controlled front organisations.

33. This may significantly complicate the I&W process by generating disparate and marginal indications that may test or exceed the limits of AI processing. It will almost certainly require a more flexible approach to warning intelligence. In the case of (3), economic warfare also overlaps with the counter-sabotage and counter-subversion tasks of counterintelligence.

34. *Human Factors and Understanding:* **A deep, well-informed intelligence analysis understanding of the leaderships and decision-making in adversary capitals needs to be co-equal with detection and collation side of I&W.** Warning assessment cannot rest solely on the automated processing of spreadsheets of machine-readable intelligence data on indications. It also requires deep, penetrative intelligence awareness of motivations, goals and *desiderata* and adversary decision processes. And this will require investment in the relevant cultural, political and contextual understanding.

Question 5: Who should be our partners of the future? Should we do things differently to influence and reassure our partners (now and in the future)? How should we prioritise?

35. **Partnership with the private sector has become more important than ever.** Private enterprise and NGOs are already significant players in intelligence: as vendors, but also as vectors for

collection, analysis, and public diplomacy. Investment in and partnership with these sectors should continue to be a priority.

36. **The Private Sector are the MOD's partners in risk and security.** Security risks in the private sector posed by hostile foreign powers (HFPs) must be solved collaboratively. The panel anticipates ongoing integration of cloud computing, AI, and web 3.0 (blockchain) into the MOD's intelligence storage, retrieval, analysis, and validation systems. Ukraine, in the middle of an existential emergency, has moved exclusively to cloud because of the security and resilience it offers (it is also cheaper). The panel viewed this shift as inevitable, and the sooner the UK adapts, the better. There are also counterintelligence opportunities to be found in firms which do not qualify for list-x/FSC. These can be targets for threats but also vectors to root them out.

37. **Our trade partners and emerging markets are natural opportunities for developing new and improved intelligence partnerships.** With reference to the discussion on countering the belt and road project, intelligence partnerships within the global south must be developed and nurtured to monitor, contain, or even counteract the PRC's expanding influence. The nurturing of new and important relationships will require investment in both attention and personnel. This requires some devotion to specialism within the FCDO and MOD. This effort could be augmented further through partnership with private entities such as defence and security consultancies.

38. **The FVEY partnership remains foundational to the UK's strengths in intelligence**. It is at least partly responsible for the UK's outsized influence in diplomatic, security, and geopolitical affairs. We would expect this to continue, however, the UK must plan contingencies for a range of adverse outcomes, especially if American policy returns toward NATO-scepticism, isolationism, or even rapprochement with powers hostile to UK interests. These plans must prepare the MOD for substantial changes in process with respect to foreign liaison. This increased burden also presents opportunities for the UK to lead intelligence partnership among democracies.

39. **The MOD's approach to international partnerships calls for a fresh perspective on vetting.** Where family ties to HFPs or states with whom we are developing closer intelligence ties are often viewed as negative, we may be excluding talent and personnel with access and knowledge to areas of interest. The MOD needs to build vetting practices that allow it to bring 1st generation migrants more easily into service, to harness their languages and cultural knowledge.

40. **The risks inherent to these partnerships come alongside opportunity for robust investment in CI.** This is an opportunity to reform vetting and list-x (FSC), so to create and exploit these opportunities. Also, a more technical (and, likely, technologically-driven) approach to information control would enable confidence within the MOD when employing and cooperating with subjects traditionally regarded as "risky."

41. **The MOD should prioritise the development of these partnerships based on capability**. These decisions must be guided by a clear picture of political (or other material) outcomes. Estonia was cited as an example of a state whose IC prioritises cooperation based on capability. This presents some cultural difficulties though, as it requires both the UK and its partners to concede their own limitations. Beyond that, naturally, the UK's priorities for intelligence partnership should be driven by the national interest and UK policy and strategy.

Question 6: What must UK Defence learn from the experiences of the War in Ukraine for its own warfighting, and what must it avoid?

42. **The UK needs to invest time in preparing for the next major conflict**. Russia's ongoing illegal invasion of Ukraine raises several important key points around the use of intelligence and other related activities. Before discussing the application of intelligence, the panel raised the point that processes and systems need to be heavily invested into well in advance of conflict. It was noted that Ukraine had a decade of support from its allies, especially the United States and UK, and Ukraine had adequate time to prepare the intelligence apparatus for the upcoming conflict. The panel also noted the importance of investing time and effort (at least a decade) in developing the European-wide partnerships with NATO/non-NATO allies to fill gaps in intelligence capability. It was suggested that investment for the future should include languages within HMG. This raised the question of horizon scanning within HMG.

43. **The UK can learn lessons from the tactical and operational use of intelligence**. While the intelligence war has been seen as one of Western success (notably FVEY and smaller NATO allies), the panel noted that Ukraine had mastered the age-old issue of Denial & Deception (D&D) in the information age. The so-called 'Kherson ruse'[6] and Kyiv's mastery of the information space provided lessons to draw on in future. Members of the panel also noted the need to delegate the assessment of information down to the tactical level to exploit opportunities as they arise, reflecting discussions here in the UK. On the Russian side, it was noted that bad operational security, combined with poor situational awareness, significantly exacerbated existing Russian tactical and operational failings on the battlefield.[7] Western assessments of Russia's military capability, while having a good understanding of the numbers of troops deployed, lacked an understanding of military effectiveness, partially driven by an absence of information on the operational/strategic culture of Russia's military. The threat of China, and continued threat posed by Russia, requires HMG to prioritise expertise on these armed forces.

44. **The release of intelligence for impact has been important**. The panel recognised the importance of using intelligence for 'impact' to counteract Russia's false narratives. Although the use of intelligence for prebuttal is dependent on using open-source information to mask 'secret' intelligence, the US/UK publication of intelligence proved key in mastering the information space, and in helping build the necessary alliances to support Ukraine.[8] DI's daily sharing of information to the public and media had shaped the narrative effectively, and there were wider lessons to be learnt in future about how such operations could be used to support future military operations.

45. **The War on Ukraine highlights the need for the UK to invest in information operations**. More widely, it was noted by the panel that the War on Ukraine offered a mixed picture for future information operations. Ukraine has managed to successfully shape the information space in the West thanks to effective propaganda campaigns through state and non-state activities, while Russia had enjoyed limited success in information activity in the Global South and elsewhere, though such activity

[6] The Kherson Ruse: Ukraine and the Art of Military Deception, December 2022 < The Kherson Ruse: Ukraine and the Art of Military Deception - Modern War Institute (usma.edu) >
[7] Intelligence and the War in Ukraine, Part II, May 2022 < Intelligence and the War in Ukraine: Part 2 - War on the Rocks >
[8] Intelligence and the War in Ukraine, Part I, May 2022 < Intelligence and the War in Ukraine: Part 1 - War on the Rocks>

in the West had limited success. The panel discussed how the UK's approach to information activity in the Global South should be revisited to rethink ways of combatting the growth of Russian activity in the form of Wagner Group, as well as wider disinformation activity.

46. **The open-source realm offers opportunities**. The role of open-source intelligence was discussed. The UK government's commitment to invest in an OSINT hub was broadly welcomed, yet questions were asked about the size, funding, and substance of the hub. Additionally, while the narrative on OSINT had dominated discussion, the panel recognised that the UK's existing machinery for secret intelligence collection and assessment continued to play a significant role. The future of OSINT raised important questions of in-house culture, attitudes to security classification and external advice for HMG, in addition to the need to avoid the replication of work across government. The information landscape had grown exponentially, even in the brief period since the start of the Syrian civil war. Since February 2022, it has been estimated that over ten years' worth of video footage had been generated in Ukraine. The scale of the OSINT problem facing HMG cannot be comprehended and is likely to require HMG to reach out beyond the traditional closed information space. Any HMG investment in OSINT would therefore have to match investment to this growth in information online.

47. **But OSINT also poses risks**. The panel noted that while OSINT is a significant potential growth area, the open-source realm opened the possibility for hostile state actors to disinform, or to collect valuable information on HMG. Therefore, the panel urge HMG to investigate counter-OSINT and to consider the negative effects of publishing information that can be exploited by hostile actors, whether within the UK or external.

Key Cross-Cutting Points Raised by Panel Members

48. **We must be more adventurous than we have allowed ourselves to be in the past.** This ties with the idea of risk avoidance versus risk management. It is also important that we not allow ourselves to fall victim to the innate caution and traditionalism of the cultures which dominate the Defence space.

49. **Expertise—real, enduring, nuanced, deep expertise—needs to be developed within MOD on regional issues and in terms of languages**. We will only be able to succeed against peer competitors in the rest of the world if the UK and MOD have a pool of officers and soldiers who have a deep understanding of local languages, customs and culture.

50. **One thing which the intelligence Community is still not good at internal digital transformation**. The intelligence community will not be able to integrate AI because data is still siloed, with integration usually technically impossible. There is a digital mobilisation which needs to happen for the intelligence community to get with 21st century standards. This will need to be supported by both resources and legislation.

51. **We need to adopt AI systems to manage the data flood of the modern era in peace and war.** The amount of data, video, audio, and other information types being produced in modern warfare greatly exceeds the ability of humans to validate and process. If we are to tap into the ubiquitous information on the modern battlefield, we will need AI-based tools to do it.

52. **Financial Intelligence (FININT) is an increasingly important function both for operations abroad and within the UK**. FININT will be important in protecting the MOD's supply chains and partners. This also means understanding block-chain technologies and Cryptocurrency, which will also have key inputs to the counterintelligence task.

53. **It is equally important to have situational awareness of and expertise in place for emerging technologies, including the rise of Web 3.0.** The luxury of mass data collection through online social media platforms like Twitter and Facebook will likely change as users will veer toward segregated, decentralized networks, with siloed access to their own data. This, coupled with the rise of deepfakes and other tools for disinformation, will likely put a strain on the intelligence community resources, particularly in the absence of AI to aid in collection, monitoring, and detection of information tampering. Web 3.0 also presents collection opportunities: public, transparent records of transactions will be vital data pools, but also have the potential to delineate black markets more clearly.

54. **Counterintelligence threaded the entire fabric of this discussion. It has been neglected and needs to be rethought and reinforced significantly.** The UK, and the MOD, need to "harden" themselves as targets for HFPs while opening up to changes which facilitates effective counterintelligence. This is both a technical issue and a culture/mindset issue but affects every facet of the panel's discussion.