Written evidence submitted by
Marina Favaro and Heather Williams, King's College London (TFP0010)

Emerging technologies present a paradox for the United Kingdom (UK). On the one hand, technology is shifting power dynamics, and if the UK fails to compete, it risks falling behind. This was reflected in the government's 2021 'Integrated Review of Security, Defence, Development and Foreign Policy', which stated, 'Keeping the UK's place at the leading edge of science and technology will be essential to our prosperity and competitiveness in the digital age.'[1] On the other hand, many of these technologies are potentially destabilising, so competing in this area could worsen the international security environment. This, too, was reflected in the Integrated Review, which pointed to, 'proliferation of potentially disruptive technologies' as a 'threat to strategic stability.'[2]

The Centre for Science and Security Studies (CSSS) at King's College London is at the forefront of research on the impact of technologies such as cyber, Artificial Intelligence (AI), and hypersonic weapons on international security. We are submitting evidence so that our research can inform UK decision-makers as they tackle this technology paradox. Recent CSSS research has explored opportunities for AI to strengthen international security,[3] the impact of social media on conflict escalation,[4] the role of emerging technologies in nuclear diplomacy,[5] potential applications of blockchain,[6] and opportunities to apply arms control to hypersonic weapons[7]. Additionally, in mid-May 2021 we will publish a major study, 'Weapons of Mass Distortion: A new approach to emerging technologies, risk reduction, and the global nuclear order', which evaluates the potential for a range of emerging technologies to destabilise an ongoing crisis involving the UK and another nuclear possessor. The study draws on an expert survey and innovative research methods.

---

[1] HM Government, 'Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy', March 2021, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf, p. 4.

[2] HM Government, 'Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy', March 2021, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf, p. 76.

[3] Jessica Cox and Heather Williams, 'The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability', The Washington Quarterly, 44:1 (2021), available at: https://www.tandfonline.com/doi/abs/10.1080/0163660X.2021.1893019

[4] Heather Williams and Alexi Drew, 'Escalation by Tweet: Managing the new nuclear diplomacy', King's College London, July 2020, available at: https://www.kcl.ac.uk/csss/assets/escalation-by-tweet-managing-the-new-nuclear-diplomacy-2020.pdf

[5] Heather Williams, 'Remaining relevant: Why the NPT must address emerging technologies', King's College London, August 2020, available at: https://www.kcl.ac.uk/csss/assets/remaining-relevant-new-technologies.pdf

[6] Lyndon Burford, 'The trust machine: Blockchain in nuclear disarmament and arms control verification', King's College London, October 2020, available at: https://www.kcl.ac.uk/csss/assets/the-trust-machine-report.pdf

[7] Heather Williams, 'Asymmetric arms control and strategic stability: Scenarios for limiting hypersonic glide vehicles', Journal of Strategic Studies, 44:6 (2019), available at: https://www.tandfonline.com/doi/abs/10.1080/01402390.2019.1627521

This research programme points to three important trends that can help answer the Inquiry's guiding questions:

1. *Emerging technologies create opportunities, along with risks*. Emerging technologies' impacts on UK foreign policy and international security will depend on specific applications and actors. Indeed, many emerging technologies have the potential to advance UK interests.
2. *Technologies that 'distort' the information space, with knock-on effects for trust and online civic culture, are particularly concerning.* This includes deep fake technology, satellite jamming, and satellite spoofing, which increase the 'fog of war' and might increase the risks of escalation during a crisis.
3. *The UK should seek to lead by building partnerships and by promoting transparency.* We recommend the UK focus on partnering with the private sector, NATO allies, and the United States, particularly to reduce risks associated with disinformation. Considering the unique threats of emerging technologies to nuclear stability, we also recommend the UK use a variety of international forums to promote transparency.

This sumbission examines each of these main points in turn and includes specific recommendations for how the UK can respond to the opportunities and challenges presented by these technologies. We recognise that this Inquiry is interested in a wide range of issues relating to technology and the future of UK foreign policy. Our evidence is largely focused on understanding the impact of emerging technologies on UK diplomacy, engagement with private companies on specific technological threats, and how the UK can leverage its alliances and other partnerships to shape the management of these technologies. While much of our research relates to the intersection of emerging technologies and nuclear weapons, it also offers insights that can apply to a wider range of challenges.

Emerging Technologies Create Opportunities

It is important not to treat 'emerging technologies' as a broad risk category. Most of the scholarship on emerging technologies suggests they will have a destabilising effect. This concern is particularly pronounced when it comes to nuclear weapons. For example, numerous scholars have raised concerns that the application of AI to nuclear command and control could increase risks of misunderstanding and misperceptions during a crisis.[8] An additional concern is that anti-satellite capabilities or cyber-attacks could target command and control systems, potentially leading to an 'entanglement' scenario whereby an adversary unintentionally escalates a conventional war past the nuclear threshold.[9] These technological threats were cited in the Integrated Review, as previously mentioned, as justification for changes to the UK nuclear stockpile.[10]

[8] James Johnson, 'Artificial Intelligence in Nuclear Warfare: A Perfect Storm of Instability?', The Washington Quarterly, 43:2 (2020), available at: https://www.tandfonline.com/doi/abs/10.1080/0163660X.2020.1770968

[9] James M. Acton, 'Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War, International Security, 43:1 (2018), available at: https://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320

[10] Heather Williams, 'U.K. Nuclear Weapons: Beyond the numbers', War on the Rocks, April 6, 2021, available at: https://warontherocks.com/2021/04/u-k-nuclear-weapons-beyond-the-numbers/

But technology is neither necessarily 'good' nor 'bad.' Rather, its impact on UK national security interests ultimately depends on its specific application. AI, for example, might be used for early warning and detection or arms control verification and contribute to security. Additionally, many emerging technologies are being developed in the private sector, by multinational companies that are not part of the traditional defence industrial model. The UK's Defence and Security Accelerator (DASA) affirms that, 'technological innovation is now more likely to come from the private sector, from companies based in other countries, outside of government's control, and where the interests of one government or another are of very minority interest.'[11] This development has the potential to decrease the public sector's awareness of, or control over, how new technologies mature and are applied. It would be impossible for the UK to ignore the existence of threats in the cyber domain or revert to a pre-AI era. Rather, a more tailored approach to specific applications of these technologies can help to identify the most concerning technologies, along with opportunities for leveraging them for the public good.

Technologies that 'Distort' are Potentially the Most Destabilising

Putting aside the benefits of innovation, the UK should also ask the question: Which technologies have the greatest impact on power shifts and are potentially destabilising? To answer this question, we conducted a survey of 61 experts to identify which technologies are potentially most impactful in a crisis, and which technologies are most likely to be developed by the UK and other international actors, over the next ten years.[12]

This study shortlisted ten technologies based on their ability to impact the UK's strategic objectives in the next ten years:[13] AI-powered cyber operations, hypersonic missiles, Rendezvous and Proximity Operations, satellite jamming and spoofing systems, directed energy weapons, swarm robotics, AI for Intelligence Surveillance and Reconnaissance (ISR), small satellites ('smallsats') for ISR, and deep fake technology. For each of the shortlisted technologies, experts assigned numerical values representing different aspects of crisis stability[14] (e.g., ability to deliver a disarming first strike, ability to increase dis- and misinformation), as well as barriers to development for the UK and other international actors (e.g., budgetary, human, regulatory, ethical, legal, technical). In total, 61 subject-matter experts responded to a technology survey. The data generated by this technology scoring exercise points to four technology 'clusters',[15] identified based on their impact on crisis stability: 1) distort; 2) compress; 3) thwart; and 4) illuminate, represented in Table 1: Technology Clusters.[16]

---

[11] Defence and Security Accelerator, 'Future technology trends in security', available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/728113/Future_trends_research_V6.pdf

[12] Marina Favaro, 'Weapons of Mass Distortion: A new approach to emerging technologies, risk reduction, and the global nuclear order', King's College London, forthcoming.

[13] A range of methods were used to shortlist the technologies, including a literature review, key informant interviews, a proof-of-concept study, and Red Teaming.

[14] In the nuclear weapons literature, crisis stability refers to a scenario in which 'emotion, uncertainty, miscalculation, misperception, or the posture of forces' do not incentivise leaders 'to strike first, to avoid the worse consequences of incurring a first strike'. Source: Glenn A. Kent, David E. Thaler, 'First-Strike Stability: A Methodology for Evaluating Strategic Forces', RAND Project Air Force, August 1989, available at: https://www.rand.org/pubs/reports/R3765.html

[15] The technology clusters were identified using Machine Learning k-means clustering. The data was ascertained from a technology scoring exercise, which tasked subject-matter experts (n=61) with assessing the *impact* of a given technology, as well as any barriers to its *implementation* in the UK context. The technology scoring exercise was

Table 1: Technology Clusters

	Name	Impact	Feasibility of implementation	Technologies
Cluster 1	"Distort"	Higher	Higher	Satellite jamming and spoofing
				Deep fake technology
Cluster 2	"Compress"	Higher	Lower	Hypersonic missiles
				Swarm robotics
				Kinetic ASAT weapons
				AI-powered cyber operations
				Rendezvous and Proximity Operations
Cluster 3	"Thwart"	Lower	Lower	Directed energy weapons
Cluster 4	"Illuminate"	Lower	Higher	AI for ISR
				Smallsats for ISR

Based on the survey results, we identify technologies that 'distort' as both the most impactful and most likely to be developed by the UK and other international actors. These technologies have the potential to increase the 'fog of war' by disabling or spoofing information systems, along with command, control, and communications, during a crisis. One particularly concerning application is the use of deep fake technology to undermine public trust in the quality of information; embarrass or blackmail elected officials or individuals with access to classified information; or compromise a state's classified data feeds, thereby sowing distrust in the intelligence community's conclusions.

A recent study by CSSS, 'Escalation by Tweet: Managing the New Nuclear Diplomacy', found that democracies with open societies and a free press were asymmetrically vulnerable to disinformation campaigns via social media. That same report recommended that the US Government develop interagency best practices, build societal resilience to disinformation campaigns, and improve understanding of how different states use social media platforms.[17] All

specifically designed to evaluate technologies from the perspective of UK decision-makers. More information on the research methods can be found in the forthcoming paper: 'Weapons of Mass Distortion: A new approach to emerging technologies, risk reduction, and the global nuclear order' by Marina Favaro.

[16] The use of Machine Learning to cluster the technologies sets this study apart from that which came before it. Whereas prioritisation uses the mean (or average) of all impact and implementation scores (wherein each criterion is weighted equally), clustering groups of technologies that scored similarly across various criteria. To work off the mean of the impact and implementation scores would generate a priority list of most-to-least impactful technologies but would lose the detail of *how* the technologies impact crisis stability. Clustering is a less prescriptive approach than prioritisation because it allows policymakers to decide the relative weight that they will ascribe to each criterion (i.e., are they more concerned with technologies that will impact crisis stability variable X or crisis stability variable Y?). Moreover, clustering the technologies generates meaningful policy outputs by preserving more nuance in the expert scores.

[17] Heather Williams and Alexi Drew, 'Escalation by Tweet: Managing the new nuclear diplomacy', King's College London, July 2020, available at: https://www.kcl.ac.uk/csss/assets/escalation-by-tweet-managing-the-new-nuclear-diplomacy-2020.pdf

of these recommendations are equally applicable to the UK. The report's conclusion, in 280 characters or less, was: 'To manage escalation during crises, stop tweeting.'

Technologies that 'distort' are neither particularly complex nor difficult to deploy. Any smartphone user can create and disseminate seemingly authentic deep fake videos in seconds. Satellite jamming and spoofing technologies are used by a range of state and non-state actors, particularly to disrupt GPS systems. Managing the risks associated with these technologies will require a different approach to national security by partnering with a wider range of actors and leading by example.

The UK Can Lead on Transparency Alongside Key Partners

We recommend that the UK play a leadership and entrepreneurial role in managing the risks associated with new technologies. While our recommendations focus on the wider security environment, great power competition, and the intersection of technology with nuclear weapons, many of these recommendations can apply to other scenarios. We suggest that the UK should focus on three main partnerships—private sector, NATO, and the United States—and three nuclear-related forums—the Nuclear Non-Proliferation Treaty (NPT), the P5 process, and the Creating an Environment for Nuclear Disarmament (CEND) initiative.

Partners

As discussed, many of these emerging technologies will be primarily developed in the private sector, often by companies that traditionally have not worked within defence. The public sector must therefore be able to clearly communicate with the private sector in the UK around the potential harms of dual-use technologies and explain why it may be worthwhile for non-traditional defence suppliers to consider the security needs of the society. To counter the most harmful applications of deep fake technology, the UK could design legislation to prohibit certain uses of a 'digital replica' of a person. Example of this include deep fake pornography, which could result in sanctions such as jail time.[18] This would align the UK's efforts to combat disinformation with proposed bills in the US Congress that attempt to prohibit malicious deep fakes.[19] Furthermore, the Foreign, Commonwealth, and Development Office should bring together key actors from the public and private sector to ensure that the UK is prepared for the challenges posed by technologies that damage public trust. One example of this is the Coalition for Content Provenance and Authenticity, which focuses on the development of open, global technical standards to channel content provenance efforts, including specifications and standards for social and media platforms. In the future, expertise should also be drawn from existing open-source intelligence communities and media forensics communities, as well as systems thinkers,

[18] Analysis from Deeptrace found that in 2019 non-consensual deep fake pornography accounted for 96% of the total deep fake videos online. Given that many deep fake bots are exclusively trained on databases of women, disinformation scholar Nina Jankowicz makes the case that 'women's participation in our representative democracy is at stake.' Source: Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, 'The State of Deepfakes', Deeptrace, September 2019, available at: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf; Nina Jankowicz, 'Opinion The threat from deepfakes isn't hypothetical, Women feel it every day,' *The Washington Post*, March 25, 2021, available at: https://www.washingtonpost.com/opinions/2021/03/25/threat-deepfakes-isnt-hypothetical-women-feel-it-every-day/

[19] Karen Hao, 'Deepfakes have got Congress panicking. This is what it needs to do.', MIT Technology Review, June 12, 2019, available at: https://www.technologyreview.com/2019/06/12/134977/deepfakes-ai-congress-politics-election-facebook-social/

cognitive scientists, and affected communities. Finally, better data sharing will accelerate the refinement of tools that can detect deep fakes.

In the space domain, space situational awareness (SSA) provides an understanding of the operational environment. There is currently no single provider for global SSA oversight, which introduces the possibility of conflicting information.[20] The potential risks and challenges of satellite and space debris monitoring were most recently evident with the uncontrolled atmospheric re-entry of a Chinese rocket body.[21] This is a reminder of the larger problem of orbital debris, which increases the likelihood of future collisions and could render parts or entire orbits unusable for future space activities. Given the increasing number of both public and private space operators and congestion in space, the UK should develop a nationally assured SSA capability and trusted process. This could be as simple as two strategically placed radars (e.g., one in the Falklands and the second in Northern Scotland), which would provide support to UK's the ability to monitor objects in low Earth orbit. The UK should develop this as a civil programme because it is easier to share civilian data with the military than the other way around. This could augment the Allied Space Surveillance Network, which is global in scope, but cannot share data behind the 'military firewall' and is optimised for missile warning, rather than SSA.[22] A nationally assured SSA capability will be critical to the UK's mission of 'enhanc[ing] space sustainability and maintain[ing] the UK space industry as a global leader'.[23]

More broadly, the UK should partner with private companies that are driving innovation, provide incentives to recruit into government from the private sector, and create new formats of engagement so that policymakers and scientists/technologists can come together and discuss emerging technologies and their interconnections.

Second, NATO remains a key partner for the UK in maintaining a technological edge and reducing risks associated with emerging technologies. In a speech from February 2021, NATO Secretary General Jens Stoltenberg warned that a 'technological gap between allies' could impede interoperability.[24] Stoltenberg recommended the development of common standards and ethical guidelines for the use of many of these technologies. In the context of nuclear weapons, NATO Director of Nuclear Policy, Jessica Cox, highlighted that, 'the advancement of new technologies … poses inherent risks to nuclear deterrence and the way we conduct our nuclear business.'[25] NATO members should individually and jointly commit to keep a 'human in the

---

[20] Bruce McClintock, Katie Feistel, Douglas C. Ligor, and Kathryn O'Connor. 'Responsible Space Behaviour for the New Space Era: Preserving the Province of Humanity', RAND Corporation, 2021, available at: https://front.un-arm.org/wp-content/uploads/2021/04/rand-pea887-2.pdf

[21] Leonard David, 'Falling Uncontrolled from Space, Giant Chinese Rocket Highlights Risk of Orbital Debris', *Scientific American*, May 6, 2021, available at: https://www.scientificamerican.com/article/falling-uncontrolled-from-space-giant-chinese-rocket-highlights-risk-of-orbital-debris/

[22] Joint Air Power Competence Centre, 'Command and Control of a Multinational Space Surveillance and Tracking Network', June 2019, available at: https://www.japcc.org/wp-content/uploads/JAPCC_C2SST_2019_screen.pdf

[23] UK Space Agency, Ministry of Defence, and Department for Business, Energy & Industrial Strategy, ''Government backs UK companies tackling dangerous 'space junk'', September 16, 2020, available at: https://www.gov.uk/government/news/government-backs-uk-companies-tackling-dangerous-space-junk

[24] Vivienne Machi, 'NATO leader: Allies must avoid capability gaps while investing in disruptive tech', *DefenceNews*, February 15, 2021, available at: https://www.defensenews.com/global/europe/2021/02/15/nato-leader-allies-must-avoid-capability-gaps-while-investing-in-disruptive-tech/

[25] 'Rising nuclear risk, disarmament, and the Nuclear Non-Proliferation Treaty', UK House of Lords Select

loop' in nuclear decision-making, as a matter of priority. It should also work to combat disinformation campaigns, both in the public realm, such as on social media platforms, and in military intelligence, in partnership with the private sector where possible, across all NATO countries.

And third, as the UK's closest ally and a global technology leader, the United States must be a partner for all these efforts going forward. The March 2021 Interim US National Security Guidance clearly aligns with the priorities of the UK and this Inquiry: 'Emerging technologies remain largely ungoverned by laws or norms designed to center rights and democratic values, foster cooperation, establish guardrails against misuse or malign action, and reduce uncertainty and manage the risk that competition will lead to conflict.'[26] The Biden Administration is clearly committed to strengthening America's technological infrastructure. The Administration also shares the UK's concerns about the potentially destabilising impact of technologies such as AI on international security and nuclear stability; therefore, the two should partner to promote transparency in nuclear doctrines and modernisation to reduce risks of misperception and crisis escalation.

Forums for Transparency

The UK has an opportunity to be an international leader on emerging technologies, and transparency should be central to its approach. The Integrated Review, for example, struck a delicate balance of 'deliberate ambiguity' and transparency in how the UK will respond to new military technologies that threaten to undermine strategic stability. This balance is not easy. Like other states, the UK must protect its businesses and intellectual property, indicating the limitations of transparency. Our recommendations focus on how the UK can promote transparency around emerging technologies specifically as they relate to nuclear weapons. This aligns with a 2019 House of Lords Inquiry, which pointed to emerging technologies as a main contributor to rising nuclear risks.[27]

First, the UK can use its legacy as a leader in transparency within the NPT to encourage other nuclear possessors to be equally transparent in their own nuclear doctrines. The NPT, often seen as the cornerstone of the nuclear order, is increasingly polarised by lack of progress towards nuclear disarmament. Cooperation on emerging technologies and nuclear risk reduction offers an important and timely opportunity for nuclear possessors and non-possessors to work towards achieving the Treaty's ultimate goals of disarmament, non-proliferation, and peaceful uses of nuclear energy. The UK should continue to pursue verification partnerships with non-nuclear weapon states—as it has with Norway—and expand the nature of these collaborations with states such as Estonia and the Netherlands, who have specialist knowledge in cybersecurity. Such partnerships should extend beyond defence to include, for example, digital health care.[28]

Second, one unique opportunity within the NPT is the P5 process, which the UK established in 2008. The P5 process brings together the five recognised nuclear possessors (China, France,

---

Committee on International Relations, April 24, 2019, available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldintrel/338/33803.htm

[26] https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf, pp. 8-9.

[27] https://publications.parliament.uk/pa/ld201719/ldselect/ldintrel/338/338.pdf

[28] https://london.mfa.ee/estonian-and-british-pms-discussed-defence-cooperation-and-digitalisation-in-london/

Russia, the United States, and United Kingdom) to make progress towards nuclear disarmament. At the most recent full P5 meeting, hosted in London in February 2020, the UK was one of the leading voices calling for increased discussion of emerging technologies and their impact on nuclear stability. Emerging technologies are now a regular agenda item for the P5 process. Ideally, these conversations would lead to the development of near-term politically-binding confidence-building measures that can help create and sustain mutual understanding and trust between P5 members. This could include regular dialogue, information sharing, best practice exchanges, and scientific cooperation programmes. Such agreements might resemble historical efforts to avoid misperceptions during crises, such as the 1972 Incidents at Sea Agreement, but making progress on risk reduction around these technologies will also require new thinking and mechanisms.

Finally, in 2019 the United States launched a new initiative on nuclear disarmament, which provides a unique forum and opportunity for leading on transparency and managing the risks of emerging technologies in the context of nuclear weapons. The Creating an Environment for Nuclear Disarmament (CEND) initiative is an informal Track 1 dialogue with dozens of state participants working on three main topics: 1) reducing reliance on nuclear weapons; 2) mechanisms and institutions; and 3) risk reduction. The working groups are co-chaired by Morocco and the Netherlands, South Korea and the United States, and Finland and Germany respectively. The challenges and opportunities associated with emerging technologies cut across all three of these areas. The UK should act as a bridge between the P5 process and CEND to identify which technologies have the most potential to increase nuclear risks, encourage greater transparency on the part of other nuclear possessors, and lead a multilateral effort to promote norms around these technologies.

Conclusions

This submission makes three key points. First, policymakers and scholars alike should avoid a defeatist attitude as regards emerging technologies. UK decision-makers should be thinking about how to mitigate the risks associated with emerging technologies, while remaining cognisant of the potential benefits of innovation. Second, UK decision-makers should be thinking about the ability of emerging technologies to escalate crises in non-linear ways. Deep fake technologies, as well as satellite jamming and spoofing capabilities, are likely to distort the information space, which could escalate a crisis to include the use of nuclear weapons. Third, the UK should continue to work closely with NATO allies and the United States, whilst broadening its partnerships with the private sector.

Dr Heather Williams is a Lecturer in the Centre for Science and Security Studies at King's College London. She is currently a Stanton Nuclear Security Fellow at the Massachusetts Institute of Technology (MIT). Her research focuses on arms control and emerging technologies, the global nuclear order, and social media and nuclear escalation.

Marina Favaro is a Research Fellow at IFSH Hamburg and a Consultant at King's College London. Her research focuses on the impact of emerging technologies on arms control. She has expertise in several qualitative and quantitative research methods, including futures and foresight methods.

May 12, 2021